大学

数学系

自学丛书

近世代数



JINSHI DAISHU

大学数学系

自学丛书

空间解析几何	高等几何
高等代数	计算方法
数学分析	概率论与数理统计
常微分方程	近世代数
复变函数论	微分几何
实变函数论	电子计算机与算法语言BASIC

统一书号：7090·299

定　　价：2.85 元

大学数学系自学丛书

近世代数

东北师范大学
高绪珏　主编

辽宁人民出版社

近世代数

Jinshi Daishu

高绪珏 主编

辽宁人民出版社出版　　辽宁省新华书店发行

（沈阳市南京街6段1里2号）　　朝阳六六七厂印刷

字数：380,000　　开本：850×1168 $\frac{1}{32}$　　印张：14$\frac{3}{8}$

印数：1—14,000

1985年5月第1版　　1985年5月第1次印刷

责任编辑：俞晓群　　封面设计：安今生

统一书号：7090·299　　定价：2.85 元

出 版 说 明

为了适应广大在职人员和社会青年自学成才的需要，根据国家建立高等教育自学考试制度的精神，以满足学员自学教材的要求，由辽宁人民出版社出版一套大学数学系自学丛书。

本丛书是由东北师范大学数学系，根据教育部规定的普通高等院校本科必修课现行教学计划和教学大纲编写的。教材内容系统，数据充实，条理清晰，深入浅出；每章均有学习指导和习题解答，便于自学。经过刻苦自学，即可无师自通，达到本科毕业水平。

本丛书有：空间解析几何、高等代数、数学分析、高等几何、常微分方程、复变函数论、近世代数、实变函数论、微分几何、计算机与算法语言BASIC，概率论与数理统计、计算方法等。本丛书既可供自学应试之用，也可供大专院校的本科在校生和函授生及业余大学学生使用。

本丛书由于水平所限，不当之处在所难免，我们热诚希望广大自学读者批评指正。

目　　录

第一部分　近世代数……………………………………………………1

第一章　基本概念……………………………………………………1

§1　集合……………………………………………………1

§2　映射……………………………………………………5

§3　商集与等价关系……………………………………………………15

§4　代数体系……………………………………………………22

§5　同态　同构……………………………………………………30

§6　半群　亚群……………………………………………………34

第二章　群……………………………………………………42

§1　群的定义……………………………………………………42

§2　子　群……………………………………………………52

§3　群的同态、同构……………………………………………………58

§4　循环群……………………………………………………63

§5　变换群　置换群……………………………………………………70

§6　子群的陪集……………………………………………………75

§7　正规子群与商群……………………………………………………82

§8　群的同态基本定理……………………………………………………89

§9　直和……………………………………………………95

第三章　环与域……………………………………………………99

§1　环的定义……………………………………………………99

§2　整环、除环和域……………………………………………………103

§3　子　环…………………………………………………… 107
§4　矩阵环…………………………………………………… 113
§5　理想与商环（差环）………………………………… 118
§6　环的同态与同态基本定理………………………… 125
§7　极大理想与素理想…………………………………… 133
§8　商　域…………………………………………………… 136
§9　多项式环………………………………………………… 141
§10　整环和域上的多项式环…………………………… 147
§11　唯一分解环…………………………………………… 154

第四章　模…………………………………………………… 164
§1　模的定义………………………………………………… 164
§2　模的生成集……………………………………………… 172
§3　自由模…………………………………………………… 176
§4　n秩自由模上的线性代数………………………… 184
§5　向量空间上的线性代数……………………………… 195
§6　子模和商模……………………………………………… 208
§7　态射……………………………………………………… 215

第五章　扩　域……………………………………………… 223
§1　特征数　素域…………………………………………… 223
§2　扩　张…………………………………………………… 227
§3　单纯扩张………………………………………………… 232
§4　有限扩张………………………………………………… 238
§5　分裂域…………………………………………………… 243
§6　有限域…………………………………………………… 248

第二部分　近世代数学习指导……………………………… 254

第一章　基本概念学习指导………………………………… 255
第二章　群学习指导………………………………………… 269

第三章　环与域学习指导…………………………………… 301
第四章　模学习指导………………………………………… 328
第五章　扩域学习指导……………………………………… 349

第三部分　近世代数习题解答……………………………… 366

第一章　基本概念习题解答………………………………… 366
第二章　群习题解答………………………………………… 378
第三章　环与域习题解答…………………………………… 404
第四章　模习题解答………………………………………… 430
第五章　扩域习题解答……………………………………… 455

附　录………………………………………………………… 467

后　记………………………………………………………… 468

第一部分　近世代数

第一章　基本概念

在这一章里，我们将介绍学习这门课程的预备知识以及近世代数的几个最基本的概念．近世代数的主要研究对象是代数体系，而代数体系是建立在集合概念基础之上的，所以我们从集合谈起．

§1　集　　合

人们观察某种客观事物，其观察对象一般总是隶属于某一确定的范围，所有观察对象都在该范围之内，而在该范围之外的则都不是．例如我们调查一个班级的学生的健康情况，那么这个班的每个学生都是调查对象；这个班以外的人都不是调查对象．我们把某一范围内的对象全体叫做一个**集合**，组成一个集合的每个对象叫做这个集合的**元素**（或元）．于是一个班级的学生全体是一个集合，这个班级的每个学生都是这个集合的元素．今后我们用大写拉丁字母A、B、C、…表示集合，小写拉丁字母a、b、c、…表示元素．当a是集合A的元素时，记为$a\in A$（读作a属于A）或$A\ni a$（读作A含着a）．当a不是A的元素时，记为$a\overline{\in}A$（读作a不属于A）或$A\overline{\ni}a$（读作A不含着a）．

我们在以前的学习中，已经接触过大量的集合．例如：全体自然数组成一个集合，叫做自然数集，记为N；全体整数组

成一个集合，叫做整数集，记为$\boldsymbol{Z}$；全体有理数组成一个集合，叫做有理数集，记为$\boldsymbol{Q}$；全体实数组成一个集合，叫做实数集，记为$\boldsymbol{R}$；全体复数组成一个集合，叫做复数集，记为$\boldsymbol{C}$。

数域F上的全体n阶方阵组成集合$M_n(F)$，数域F上的全体多项式组成集合$F[x]$。

自然，四个数码1，2，3，4组成一个集合，甲、乙两个人组成一个集合。一般地，由有限个元素组成的集合叫做**有限集**；由无限多个元素组成的集合叫做**无限集**。

对于一个集合A来说，如果能够把A的每个元素都确定出来，那么集合A就确定了。于是有时我们用列举A的所有元素的方法表记A。例如A是由元素a，b，c组成的，则将A表为

$$A=\{a, b, c\}$$

或

$$A \vdots a, b, c$$

其中花括号里或"⋮"之后列入A的全部元素。当元素过多不便全部列入时，则先列入A的部分元素，再用删节号表示其余元素。比如可将自然数集N表为

$$N=\{1, 2, 3, \cdots\}$$

$$N \vdots 1, 2, 3, \cdots$$

表示集合的另一种方法，是通过这个集合的元素所具有的属性去表示它。当集合A的每个元素都满足某个条件，而且不属于A的元素都不满足这个条件时，可用这个条件描述A。

$$A=\{\triangle \mid \boxed{\quad}\}$$

其中位置△记入表示A的元素的字母，位置$\boxed{\quad}$记入A的元素所满足的条件。如

$$A=\{x \mid x\in R, x^2-2=0\}$$

表明A是由满足方程式$x^2-2=0$的全体实数组成的集合，即二次方程$x^2-2=0$的所有实根的集合，亦即$A=\{\sqrt{2}, -\sqrt{2}\}$。

为了减少冗长叙述，有时采用下列记号："$\forall$"，读作"对于每个"，"$\Longrightarrow$"，读作"推得"，"$\Longleftrightarrow$"，读作"必

要而且只要”。这些记号也可读作其他的同义语。

设A，B是两个集合，如果A的每个元素都属于B，则说A是B的**子集**，记为$A\subseteq B$（读作：A含在B里）或$B\supseteq A$（读作：B包含着A）。当A不是B的子集时，记为$A\nsubseteq B$。

显然$A\subseteq B \Longleftrightarrow \forall a\in A$有$a\in B$。例如$N$是$Z$的子集，$Z$也是$Z$的子集。

如果$A\subseteq B$且$B\subseteq A$，则说A与B**相等**，记为$A=B$。显然$A=B\Longleftrightarrow \forall a\in A$有$a\in B$，而且$\forall b\in B$有$b\in A$。

如果$A\subseteq B$且$A\neq B$，则说A是B的**真子集**，记为$A\subset B$。显然$A\subset B\Longleftrightarrow \forall a\in A$有$a\in B$，而且存在$b\in B$，使得$b\notin A$。例如$N$是$Z$的真子集。

定义1 不含任何元素的集合叫做空集，记为ϕ。规定ϕ是任一集合的子集。

例如，多项式$f(x)=x^2-2$的有理根的集合，速度超过光速的飞机的集合都是空集。

设A，B是两个集合，则由一切既属于A又属于B的元素组成的集合叫做A与B的**交**，记为$A\cap B$。即$A\cap B=\{x|x\in A$且$x\in B\}$。易证，$A\cap B=A\Longleftrightarrow A\subseteq B$。事实上，如果$A\cap B=A$，则$\forall a\in A$有$a\in A\cap B$，从而$a\in B$，故$A\subseteq B$。反之，如果$A\subseteq B$，则一方面$\forall b\in A\cap B$有$b\in A$；另一方面$\forall c\in A$有$c\in B$，从而$c\in A\cap B$。于是$A\cap B=A$。

当$A\cap B\neq\phi$时，则说A与B**相交**；当$A\cap B=\phi$时，则说A与B**不相交**。

设A，B是两个集合，则由一切属于A或者属于B的元素组成的集合叫做A与B的**并**，记为$A\cup B$，即$A\cup B=\{x|x\in A$或$x\in B\}$。

易证：$A\cup B=B\Longleftrightarrow A\subseteq B$。（证明留给读者）。

设A，B是两个集合，则由一切属于B但不属于A的元素组成的集合叫做A在B中的**余集**，记为$B\backslash A$，即$B\backslash A=\{x|x\in B$而$x\notin A\}$。

当$A\subseteq B$时，$B\backslash A$叫做A在B中的补集，此时，把$B\backslash A$记为A'.

显然，$A\cup A'=B$，$A\cap A'=\phi$.

例如，设$A=\{1,2\},B=\{1,3,4\},C=\{3,4\}$ 时，则$A\cap B=\{1\}$，$A\cup B=\{1, 2, 3, 4\}$，$B\backslash A=\{3, 4\}$. C是B的子集，C在B中的补集$C'=\{1\}$. A与B相交，A与C不相交. 请注意集合$\{1\}$，它是由一个元素1组成的. 集合$\{1\}$和元素1有区别，对B来说，$\{1\}$是B的子集：$\{1\}\subset B$，而1是B的元素：$1\in B$.

集合A的一切子集所组成的集合叫做A的幂集，记为$P(A)$，即 $P(A)=\{X|X\subseteq A\}$. 这里要注意，X在A中是子集合，X在$P(A)$中则是元素. 例如，$A=\{1, 2, 3\}$，则$P(A)=\{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$.

设A，B是两个集合，则A的每个元素a与B的每个元素b所做成的序对 (a, b)的全体叫做A与B的笛卡尔（Descartes）积，记为 $A\times B$，即 $A\times B=\{(a, b)|a\in A, b\in B\}$. 例如，$A=\{a, b, c\}$，$B=\{x, y\}$，则 $A\times B=\{(a, x), (a, y), (b, x), (b, y), (c, x), (c, y)\}$. 实数集（实数轴）$R$与其自身的笛卡尔积$R\times R$就是实平面全体点的集合.

设 $A_1, A_2, \cdots, A_n$ 是n个集合，则它们的笛卡尔积是$A_1\times A_2\times\cdots\times A_n=\{(a_1, a_2,\cdots,a_n)|a_i\in A_i, i=1,2,\cdots,n\}$.

集合的交和并概念可推广到任意多个集合的情形. 为了容易分清层次，有时把由集合做为元素所组成的集合叫做族. 例如，A的幂集$P(A)$就是A的所有子集族. 设$\{A_i|i\in I\}$是任一集合族，其中每个A_i都是集合，I是所有A_i的下标的集合. 于是这个集合族的交（记作$\bigcap_{i\in I}A_i$）规定为

$$\bigcap_{i\in I}A_i=\{x|\forall i\in I:x\in A_i\}$$

这个集合族的并（证作$\bigcup_{i\in I}A_i$）规定为

$$\bigcup_{i\in I}A_i=\{x|存在i\in I使x\in A_i\}$$

习　　题

1　设 $A=\{1,2,3,4\}$，$B=\{2,4,6,8\}$，$C=\{2,4\}$。写出 $A\cap B$，$A\cup B$，$A\setminus B$，$B\setminus A$，$P(A)$以及C分别在A和B中的补集。

2　设A，B，C都是集合，证明下列等式。

（1）幂等律：$A\cap A=A$，$A\cup A=A$

（2）结合律：$(A\cap B)\cap C=A\cap(B\cap C)$

$(A\cup B)\cup C=A\cup(B\cup C)$

（3）交换律：$A\cap B=B\cap A$，$A\cup B=B\cup A$

（4）分配律：$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$

$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$

（5）吸收律：$A\cup(A\cap B)=A$，$A\cap(A\cup B)=A$

§2　映　　射

上节讨论了集合的概念．在我们的研究中所遇到的一些集合往往不是孤立的，它们之间存在着各种各样的关系。现在我们来讨论在两个集合之间建立联系的一种手段——映射。

定义1　对于给定的集合A和B，如果存在一个法则φ，通过它，A中的每个元素a，都在B中确定唯一的元素a'，则法则φ叫做A到B的一个映射，记为

$$\varphi:\ A\longrightarrow B \text{ 或 } A\xrightarrow{\varphi}B$$

A叫做φ的定义域，B叫做φ的值域。元素a'叫做a在φ之下的象，a叫做a'在φ之下的一个原象，记为

$$\varphi:\ a\longmapsto a' \text{ 或 } \varphi(a)=a'$$

例1　设 $y=f(x)$是定义在$[0,1]$上的实值函数。这是集合$[0,1]$到实数集R的一个映射，用我们现在的表示法就是f：$[0,1]\longrightarrow R$。实际上，微积分中所见到的单值函数都是映射。

例2　设$A=\{x,y,z\}$，$B=\{a,b,c,d\}$。

φ_1: $x\longmapsto a$, $y\longmapsto b$, $z\longmapsto c$

是A到B的映射．注意，d在φ_1之下无原象．它表明，映射值域中的元素不必都有原象．

φ_2: $x\longmapsto a$, $y\longmapsto a$, $z\longmapsto b$

是A到B的映射．注意，x和y的象都是a．这说明，映射的定义域中的不同元素可以有相同的象．

φ_3: $x\longmapsto a$, $x\longmapsto b$, $y\longmapsto c$, $z\longmapsto d$

不是A到B的映射．这是因为φ_3为x确定了两个不同元素a和b做为象，x的象不唯一，不符合映射定义．

φ_4: $x\longmapsto a$, $y\longmapsto b$

φ_4没有给z确定象，φ_4不是A到B的映射．

例 3 设$A=\mathbf{Z}$，$B=\{2n\mid n\in\mathbf{Z}\}$（所有偶数的集合），$\forall n\in\mathbf{Z}$定义

φ_1: $n\longmapsto 2n$

φ_2: $n\longmapsto 4n$

φ_3: $n\longmapsto n$，当$2\mid n$

$n\longmapsto n+1$，当$2\nmid n$

φ_4: $n\longmapsto |n|$，当$2\mid n$

$n\longmapsto |n+1|$，当$2\nmid n$

这四个法则都适合映射的定义，都是整数集$\mathbf{Z}$到偶数集B的映射．

例 4 设$A=M_n(F)$（数域F上所有n阶方阵的集合），$B=\{0, 1, 2, \cdots, n\}$，则

φ: $(a_{ij})\longmapsto$ 秩(a_{ij})

是$M_n(F)$到B的映射．

例 5 设$A=F[x]$（数域F上所有多项式的集合），$B_1=\{0, 1, 2, \cdots\}$，$B_2=\{-\infty, 0, 1, 2, \cdots\}$，令

φ_1: $f(x)\longmapsto \deg f(x)$

φ_2: $f(x)\longmapsto \deg f(x)$，当 $f(x)\neq 0$

$f(x)\longmapsto -\infty$，当 $f(x)=0$

由于零多项式$f(x)=0$在φ_1之下无象，所以φ_1不是$F[x]$到B_1的映射。而φ_2是$F[x]$到B_2的映射。

例 6 设$A=B$，$\forall a\in A$令

$$\varphi: a\longmapsto a$$

则φ是A到A的一个映射。此映射叫做A的恒等变换，通常用I_A表示A的恒等变换。

设φ是A到B的映射，$S\subseteq A$，则称集合$T=\{\varphi(s)\mid s\in S\}$为$S$在$\varphi$之下的象，记为$\varphi(S)=T$。显然$\varphi(S)\subseteq B$。特别地，当$S=A$时，$\varphi(A)$叫做映射$\varphi$的象，记为$\mathrm{im}\varphi=\varphi(A)$。设$V\subseteq B$，则集合$U=\{u\mid\varphi(u)\in V\}$叫做$V$在$\varphi$之下的完全原象，记为$\varphi^{-1}(V)=U$。当$V=\{x\}$时，把$\varphi^{-1}(\{x\})$记作$\varphi^{-1}(x)$。显然$\varphi^{-1}(V)\subseteq A$，特别地，$\varphi^{-1}(B)=A$。请读者留意，符号$\varphi^{-1}(V)$中的$\varphi^{-1}$不表示映射，在后面另外场合还将采用这个符号，但涵义与此不同。

定义 2 设φ，ψ都是A到B的映射，如果$\forall a\in A$均有$\varphi(a)=\psi(a)$，则说映射φ与映射ψ相等，记为$\varphi=\psi$。

例如，设$A=\{0,2\}$，$B=\{0,4\}$，$\forall x\in A$令

$$\varphi_1: x\longmapsto x^2,\quad \varphi_2: x\longmapsto 2x$$

显然φ_1，φ_2都是A到B的映射。尽管从形式上看，它们是不同的，但是对这里确定的A和B来说，由于$\varphi_1(0)=0=\varphi_2(0)$，$\varphi_1(2)=4=\varphi_2(2)$，所以$\varphi_1=\varphi_2$。

映射相等的定义表明，两个映射只要定义域不同或者值域不同，它们便是不同的映射。但是为了叙述简单起见，对下述两种情况，我们做例外的约定：设φ是A到B的映射，如果S是A的真子集，则把φ也看做是S到B的映射；如果$\mathrm{im}\varphi=C$是B的真子集，则把φ也看做是A到C的映射。

定义 3 设$\varphi: A\to B$，如果$\forall a, b\in A$，$a\neq b$，有$\varphi(a)\neq\varphi(b)$，则φ叫做单射；如果$\mathrm{im}\varphi=B$，则φ叫做满射；如果φ既是单射又是满射，则φ叫做双射。

φ是单射时，表明B的每个元素在A中的原象不能多于1

个；φ 是满射时表明，B 的每个元素必在 A 中有原象；φ 是双射时，表明 A 的全体元素可与 B 的全体元素一个对一个地对应起来。特别是，当 A、B 之一是有限集时，另一个也必是有限集，而且 A 与 B 的元素个数相等。双射是一种重要映射，后面将做进一步讨论。

例 3 中的 φ_1 是双射，φ_2 是单射但不是满射，φ_3 是满射但不是单射，φ_4 既不是单射也不是满射。例 6 中的恒等变换 I_A 是双射。

定义 4 设 A，B，C 是三个集合，$\varphi: A\to B$，$\psi: B\to C$，则 A 到 C 的映射 γ：$a\longmapsto\psi(\varphi(a))$，$\forall a\in A$，叫做 φ 与 ψ 的合成，记为 $\psi\varphi=\gamma$。

例 7 设 $A=\{a, b\}$，$B=\{1, 2, 3, 4\}$，$C=\{x,y,z\}$，

$$\varphi: a\longmapsto 1,\ b\longmapsto 3$$

$$\psi: 1\longmapsto x,\ 2\longmapsto y,\ 3\longmapsto z,\ 4\longmapsto z$$

则 φ 和 ψ 分别是 A 到 B 和 B 到 C 的映射，它们的合成是

$$\psi\varphi: a\longmapsto\psi(\varphi(a))=\psi(1)=x$$

$$b\longmapsto\psi(\varphi(b))=\psi(3)=z$$

值得注意的是，不是任何两个映射都可以做合成，能做合成的两个映射必须而且只须第一个映射的值域与第二个映射的定义域相同。还应注意，为了便于计算，在合成的记号 $\psi\varphi$ 中，把第一个映射 φ 列在第二个映射 ψ 的右边。参加合成的两个映射的顺序一般不可颠倒，尽管 $\psi\varphi$ 是映射合成，但是可能 $\varphi\psi$ 无意义（ψ 的值域不等于 φ 的定义域）例 7 便是如此。有时虽然 $\varphi\psi$ 有意义，但 $\varphi\psi\neq\psi\varphi$。所以一般的映射合成不满足交换律。然而映射合成满足结合律。

定理 1 设 $A\xrightarrow{\varphi}B\xrightarrow{\psi}C\xrightarrow{\gamma}D$，则

$$\gamma(\psi\varphi)=(\gamma\psi)\varphi$$

证明 首先，由所给条件知 $\gamma(\psi\varphi)$ 和 $(\gamma\psi)\varphi$ 是具有相同定义域 A 和相同值域 D 的两个映射。

其次证明这两个映射对A的每个元素的作用效果相同。$\forall a \in A$有

$$[\gamma(\psi\varphi)](a) = \gamma[(\psi\varphi)(a)] = \gamma[\psi(\varphi(a))]$$

$$[(\gamma\psi)\varphi](a) = (\gamma\psi)(\varphi(a)) = \gamma[\psi(\varphi(a))]$$

即

$$[\gamma(\psi\varphi)](a) = [(\gamma\psi)\varphi](a)$$

由映射相等的定义得

$$\gamma(\psi\varphi) = (\gamma\psi)\varphi$$ 证完。

关于映射合成，还有两个明显的性质：其一是，$A \xrightarrow{\varphi} B \xrightarrow{\psi} C$，则当$\varphi$、$\psi$都是单射时，$\psi\varphi$ 必是单射；当φ、ψ都是满射时，$\psi\varphi$ 必是满射；从而，当φ、ψ都是双射时，$\psi\varphi$必是双射。其二是，设φ：$A \longrightarrow B$，则 $\varphi I_A = \varphi$，$I_B\varphi = \varphi$，其中I_A和I_B分别是A和B的恒等变换。

现证明，如果$A \xrightarrow{\varphi} B \xrightarrow{\psi} C$，则当$\varphi$，$\psi$都是单射时，$\psi\varphi$必是单射（其余的证明留给读者。）事实上，$\forall a, b \in A$，如果$a \neq b$，则因$\varphi$是单射，有$\varphi(a) \neq \varphi(b)$。再因$\psi$是单射，有$\psi(\varphi(a)) \neq \psi(\varphi(b))$，即 $(\psi\varphi)(a) \neq (\psi\varphi)(b)$。于是$\psi\varphi$是单射。

下面利用映射合成给出映射是双射的判定条件，为此先给出逆映射的概念。

定义 5 设φ：$A \longrightarrow B$，如果存在ψ：$B \longrightarrow A$，使得$\psi\varphi = I_A$且$\varphi\psi = I_B$，则ψ叫做φ的逆映射。具有逆映射的映射叫做可逆映射。

初等函数中的指数函数，对数函数，线性代数中的可逆线性变换，本节例 3 中的 φ_1，例 6 中的恒等变换I_A都是可逆映射。

由逆映射的定义可直接推得：若ψ是φ：$A \longrightarrow B$的逆映射，则对于任意的$a \in A$，$a' \in B$有：$\varphi(a) = a' \Longleftrightarrow \psi(a') = a$。

事实上，如果$\varphi(a) = a'$，则$\psi(\varphi(a)) = \psi(a')$，即 $I_A(a) =$

$\psi(a')$，所以，$a=\psi(a')$。反之，如果$\psi(a')=a$，则$\varphi(\psi(a'))=\varphi(a)$，即$I_B(a')=\varphi(a)$，得$a'=\varphi(a)$。

由逆映射的定义还可直接推得：如果$\varphi: A\longrightarrow B$是可逆的，则$\varphi$的逆映射唯一。

事实上，设ψ、ψ'都是φ的逆映射，则有

$$\psi\varphi=I_A=\psi'\varphi,\quad \varphi\psi=I_B=\varphi\psi'$$

于是

$$\psi=I_A\psi=(\psi'\varphi)\psi=\psi'(\varphi\psi)=\psi' I_B=\psi'$$

现把可逆映射φ的唯一的逆映射记为φ^{-1}。

由逆映射的定义还可看出，如果φ是可逆映射，那么φ^{-1}也是可逆的，而且φ就是φ^{-1}的逆映射，即

$$(\varphi^{-1})^{-1}=\varphi$$

现在我们来证明，双射与可逆映射本质上的一致性。

定理2 $\varphi: A\longrightarrow B$**是可逆映射必要而且只要**$\varphi$**是双射。**

证明 充分性。假设φ是双射，$\forall a'\in B$，当$\varphi(a)=a'$，$a\in A$，令

$$\psi: a'\longmapsto a,\ 即\ \psi(a')=a$$

下面说明ψ是B到A的映射。按上面规定，B中的元素a'在ψ之下的象是a'在φ之下的原象a。因为φ是双射，所以B中的任意元a'在A中必有原象，而且唯一。因此，ψ是B到A的映射。下面证明ψ是φ的逆映射。

显然$\psi\varphi$和I_A的定义域和值域都是A，$\varphi\psi$和I_B的定义域和值域都是B。而且，

$$\psi\varphi((a))=\psi(\varphi(a))=\psi(a')=a=I_A(a),\quad \forall a\in A$$

所以，$\psi\varphi=I_A$。$\forall a'\in B$ 有

$$\varphi\psi(a')=\varphi(\psi(a'))=\varphi(a)=a'=I_B(a')$$

故

$$\varphi\psi=I_B$$

因此ψ是φ的逆映射。

必要性．假设 φ 是可逆的，则存在逆映射 φ^{-1}，使 $\varphi^{-1}\varphi=I_A$，$\varphi\varphi^{-1}=I_B$．于是 $\forall a'\in B$，有 $\varphi^{-1}(a')=a\in A$：

$$\varphi(a)=\varphi(\varphi^{-1}(a'))=\varphi\varphi^{-1}(a')=I_B(a')=a'$$

这说明 φ 是满射．$\forall a,\ b\in A$，假设 $\varphi(a)=\varphi(b)$，则

$$\varphi^{-1}(\varphi(a))=\varphi^{-1}(\varphi(b))$$

$$\varphi^{-1}\varphi(a)=\varphi^{-1}\varphi(b),\quad I_A(a)=I_A(b),\quad a=b$$

故 φ 是单射．于是 φ 是双射，必要性得证．证完．

定理 2 表明，判断一个映射是否是可逆的，可以通过判断它是否是双射来确定．

在本节最后部分，我们讨论一类特殊的映射——定义域和值域相同的映射．

定义 6 A **到** A **的映射** φ **叫做** A **的一个变换．当** φ **分别是单射、满射、双射时，则** φ **分别叫做** A **的单（一一）变换、满变换、双变换．**

几何中的平移，旋转，位似都是变换，线性空间的线性变换，矩阵的相似变换等也都是变换，一个集合 A 的恒等变换 I_A 是 A 的双变换．

前面对于映射的讨论自然也适用于变换，特别是：A 的任意两个变换 φ、ψ 都可以做合成，而且它们的合成 $\psi\varphi$ 仍然是 A 的一个变换．在下一节，我们将看到，正是由于这个性质，合成确定 A 的所有变换集合的一个代数运算，它对研究该变换集合的代数性质将起重要作用．

如果 φ、ψ 分别都是单变换，满变换，双变换，那么 $\psi\varphi$ 也分别是单变换，满变换，双变换．

假设 φ 是 A 的变换，如果 φ 是 A 到 A 的可逆映射，则 φ 叫做 A 的**可逆变换**．φ 的逆映射 φ^{-1} 叫做 φ 的**逆变换**．由定理 2 知，φ 是可逆变换的充要条件是，φ 是双变换．

在第二章群论中，有限集合的可逆变换将反复做为例子出现，这里有必要做进一步讨论．

定理 3 设 A 是 n 元有限集合，φ 是 A 的一个变换，则 φ

是可逆变换$\Longleftrightarrow\varphi$是单变换$\Longleftrightarrow\varphi$是满变换。

证明 当φ是可逆变换，则由定理2知，φ是单的，也是满的。

另一方面，设φ是A的单变换，则$\mathrm{im}\varphi\subseteq A$是$n$个元素的集合，于是$\mathrm{im}\varphi=A$，从而$\varphi$是满变换。反之，设$\varphi$是满的，则$\mathrm{im}\varphi=A$。如果$\varphi$不是单的，必有$A$中不同元素$a,b$使$\varphi(a)=\varphi(b)$。此时，$\mathrm{im}\varphi$的元素个数必小于$n$，这与$\mathrm{im}\varphi=A$相矛盾，所以$\varphi$必是单的。总之，只若$\varphi$是单的或者是满的，那么$\varphi$就是可逆的。证完。

今后把n元有限集合A的可逆变换叫做A的**置换**，也叫做n**元置换**。对于置换，我们给出特殊的表示记号。

设 $A=\{a_1, a_2, \cdots, a_n\}$是一个$n$元有限集合，为了书写简便，把元素$a_1, a_2, \cdots, a_n$分别用1，2，…，$n$表示，于是$A=\{1, 2, \cdots, n\}$。请读者记住，这里的数码只是抽象的元素记号，去掉了它们本来的数字涵义。

设φ是A的一个置换，φ可表示成

$$\begin{aligned}\varphi: \ & 1\longmapsto\varphi(1)\\ & 2\longmapsto\varphi(2)\\ & \ \ \vdots\\ & i\longmapsto\varphi(i)\\ & \ \ \vdots\\ & n\longmapsto\varphi(n)\end{aligned}\tag{1}$$

在这里，A的每个元素i以及与它对应的象都明确地列出来，清楚地表现了置换φ。现将表（1）转置并略去“$\longmapsto$”，改写成

$$\begin{pmatrix}1 & 2 & \cdots i \cdots & n\\ \varphi(1) & \varphi(2) & \cdots\varphi(i)\cdots & \varphi(n)\end{pmatrix}\tag{2}$$

这个表同样清楚地表现了置换φ。表的第一行记入A的全部元素，在每个元素i的正下方第二行的位置上记入i的象$\varphi(i)$。

今后我们便用（2）形的表表示置换．例如

$$\varphi=\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}$$

表示是集合 $A=\{1, 2, 3, 4\}$ 的一个置换，而且 $\varphi(1)=2$，$\varphi(2)=4$，$\varphi(3)=1$，$\varphi(4)=3$。

根据映射相等的规定，上述置换的记号中的第一行，可以不按自然顺序排列，只要把相应元素的象写在下边即可．例如，上边的置换 φ 也可写为

$$\varphi=\begin{pmatrix}3&2&1&4\\1&4&2&3\end{pmatrix}$$

其次讨论置换的个数问题．设 $A=\{1, 2, \cdots, n\}$，用 S_n 表示 A 的所有置换的集合．那么 S_n 共有多少个元素呢？也就是说，A 共有多少个置换？

我们注意表（2）的第二行．由于 φ 是 A 的双变换，所以第二行恰好是由 A 的所有 n 个不同的数码（元素）组成．如果将第一行的数码按自然顺序排列：1，2，…，n，则第二行 $\varphi(1)\ \varphi(2)\cdots\varphi(n)$ 正是1，2，…，n 的一个全排列．所以 $A=\{1, 2, \cdots, n\}$ 的每个置换都各决定一个 n 元全排列，而且不同的置换所决定的排列也不同．反之，1，2，…，n 的任一全排列 $r_1r_2\cdots r_n$ 也决定 A 的一个置换 ψ

$$\psi=\begin{pmatrix}1&2&\cdots&n\\r_1&r_2&\cdots&r_n\end{pmatrix}$$

而且不同的 n 元排列所决定的置换也不同．由此得知，S_n 的元素个数恰好等于全体 n 元全排列的个数 $n!$，故 S_n 是 $n!$ 个元素的有限集合．例如，S_2，S_3，S_4 的元素个数分别是 $2!=2$，$3!=6$，$4!=24$。

最后讨论置换的合成．前边已经指出，集合 A 的任意两个可逆变换的合成仍然是 A 的可逆变换，所以任二 n 元置换的合成也仍然是 n 元置换．设 φ，$\psi\in S_n$

$$\varphi=\begin{pmatrix}1 & 2 & \cdots & i & \cdots & n\\ \varphi(1) & \varphi(2) & \cdots & \varphi(i) & \cdots & \varphi(n)\end{pmatrix}$$

$$\psi=\begin{pmatrix}1 & 2 & \cdots & j & \cdots & n\\ \psi(1) & \psi(2) & \cdots & \psi(j) & \cdots & \psi(n)\end{pmatrix}$$

则

$$\psi\varphi=\begin{pmatrix}1 & 2 & \cdots & j & \cdots & n\\ \psi(1) & \psi(2) & \cdots & \psi(j) & \cdots & \psi(n)\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & i & \cdots & n\\ \varphi(1) & \varphi(2) & \cdots & \varphi(i) & \cdots & \varphi(n)\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & \cdots & i & \cdots & n\\ \psi(\varphi(1)) & \psi(\varphi(2)) & \cdots & \psi(\varphi(i)) & \cdots & \psi(\varphi(n))\end{pmatrix}$$

怎样才能迅速地把置换$\psi\varphi$的第二行确定出来呢？以确定$\psi(\varphi(i))$为例，这是先用φ作用i得$\varphi(i)$，$\varphi(i)$在φ的第二行里可查到，它位于第一行中的i的正下方。其次是用ψ作用$\varphi(i)$得$\psi(\varphi(i))$，这只要在ψ的第一行中找到数码$\varphi(i)$，它的正下方便是$\psi(\varphi(i))$。如$j=\varphi(i)$，则$\psi(\varphi(i))=\psi(j)$。

例 8 设

$$\varphi=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix},\quad \psi=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

则

$$\psi\varphi=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

上式中的虚线表示确定 $\psi(\varphi(2))=3$ 的观察线路：$2\overset{\varphi}{\longmapsto}1\overset{\psi}{\longmapsto}3$，即$2\overset{\psi\varphi}{\longmapsto}3$。其余的$\psi(\varphi(1))=1$，$\psi(\varphi)(3))=2$也

是同样"看"出来的。再如

$$\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4&5\\2&5&4&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\5&1&4&3&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\3&2&1&4&5\end{pmatrix}$$

请读者把上述置换颠倒顺序再做合成，从中可以看出置换合成不满足交换律。

习　　题

1　设$A=\{0, 1\}$，$B=\{a, b\}$，试建立A到B的所有映射，并分别注明哪些是单射，满射，双射以及非单非满的映射。

2　设φ是双射，且$\varphi\psi$有意义。证明：ψ是单射的充分必要条件是$\varphi\psi$是单射；ψ是满射的充分必要条件是$\varphi\psi$是满射。

3　设φ是单射，且$\varphi\psi$和$\varphi\psi'$都有意义。证明：$\varphi\psi=\varphi\psi' \Longleftrightarrow \psi=\psi'$。

4　试写出S_3的所有元素，并写出每两个三元置换的合成。

§3　商集与等价关系

在我们研究某一问题时，常常需要对研究对象做分类，以便有条理地探讨它们的性质。例如生物学中把所有的生物分为两类（界）：动物界和植物界。动物界又分成十类（门），植物界分成五类（门）。门以下还要分纲、目、科、属、种等。这些分类，有助于对生物学作系统地研究。再如对整数集Z进行研究，可把全体整数分成奇、偶两类。同类整数具有许多共同的性质，掌握这些性质，自然也加深了对Z的了解。当然，对整数集Z还可做另外的分类，比如把全体整数分成正、负、零三类。

总之，对一个集合的全体元素做分类，是研究这个集合性质的一种手段。在这节里，我们将依次回答两个问题：怎样才

算对一个集合做了成功的分类；分类的依据是什么。

对一个集合A的全体元素怎样才算做了一次成功的分类呢？首先，A的每个元素都必须分在某个类里，漏掉一个元素也不算是彻底的分类；A的每个元素都必须只分在一个类里，存在分居在两类的同一个元素，不能看成是清楚的分类；最后，每个类都须含有A的元素，不含元素的类没有意义。概括上述要求，给出如下定义。

定义1　设A是任一集合，$Q\subseteq P(A)$（A的幂集），如果满足下列条件

（1）$A=\bigcup\limits_{S\in Q}S$

（2）$\forall S,\ T\in Q,\ S\neq T$，有$S\cap T=\phi$；

（3）$\phi\notin Q$.

则Q叫做A的一个商集，Q的每个元素S叫做一个类。

构造A的一个商集，就是对A的全体元素做了一次分类。

例1　对实数集$\mathbf{R}$，全体正实数集合$\mathbf{R}^+$，全体负实数集合$\mathbf{R}^-$和$\{0\}$都是$\mathbf{R}$的子集。集族$Q=\{\mathbf{R}^+,\ \mathbf{R}^-,\ \{0\}\}$满足定义1的全部条件，是$\mathbf{R}$的一个商集。

例2　设A是一个班全体学生的集合，假如这个班的学生共有四种年龄：18岁，19岁，20岁，21岁。自然可把全班学生分成四类：全体18岁的为一类T_{18}，依此类推有T_{19}，T_{20}和T_{21}；集族$Q=\{T_{18},\ T_{19},\ T_{20},\ T_{21}\}$满足商集定义的条件，是$A$的一个商集。

例3　设F为任一数域，$F[x]$是F上全体多项式集合，令

$$T_0=\{f(x)\in F[x]\mid \deg f(x)=0\}$$
$$T_1=\{f(x)\in F[x]\mid \deg f(x)=1\}$$
$$T_2=\{f(x)\in F[x]\mid \deg f(x)=2\}$$
$$\vdots$$

上述T_i都是$F[x]$的子集，但集族$\{T_0,\ T_1,\ T_2,\ \cdots\}$不是$F[x]$的商集，它不满足定义1的条件（1），这是因为零多项式不

属于任何 T_i。如果令

$$T=\{0\}$$

则 $Q=\{T, T_0, T_1, T_2, \cdots\}$是$F[x]$的一个商集。

例 4 设A是整数集$\boldsymbol{Z}$的全体变换的集合，T_1是$\boldsymbol{Z}$的所有单变换的集合，T_2是$\boldsymbol{Z}$的所有满变换的集合，T_3是$\boldsymbol{Z}$的既不单又不满的变换的集合。T_1，T_2，T_3是A的互不相同的非空子集，但是集族$\{T_1, T_2, T_3\}$不是A的商集，它不满足商集定义的条件（2），比如恒等变换$I_Z\in T_1\cap T_2$，即$T_1\cap T_2\neq\phi$。

例 5 对于整数集$\boldsymbol{Z}$设

$$\overline{0}=\{n\in\boldsymbol{Z}\mid n=3q,\ q\in\boldsymbol{Z}\}$$

即 3 的全体整倍数的集合。

$$\overline{1}=\{n\in\boldsymbol{Z}\mid n=3q+1,\ q\in\boldsymbol{Z}\}$$

即除以 3 余数为 1 的全体整数的集合。

$$\overline{2}=\{n\in\boldsymbol{Z}\mid n=3q+2,\ q\in\boldsymbol{Z}\}$$

即除以 3 余数为 2 的全体整数的集合。

容易验证，$Q=\{\overline{0}, \overline{1}, \overline{2}\}$满足商集定义中的条件，是$\boldsymbol{Z}$的一个商集。今后把对$\boldsymbol{Z}$这样分得的类$\overline{i}$叫做整数集$\boldsymbol{Z}$的以 3 为模的剩余类，同时把此商集记为$\boldsymbol{Z}_3=Q$。

一般地，可取任一正整数m，令

$$\overline{0}=\{n\in\boldsymbol{Z}\mid n=qm,\ q\in\boldsymbol{Z}\}$$

$$\overline{1}=\{n\in\boldsymbol{Z}\mid n=qm+1,\ q\in\boldsymbol{Z}\}$$

$$\vdots$$

$$\overline{m-1}=\{n\in\boldsymbol{Z}\mid n=qm+(m-1),\ q\in\boldsymbol{Z}\}$$

记$\boldsymbol{Z}_m=\{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$，它是$\boldsymbol{Z}$的一个商集，其中每个类$\overline{i}$叫做整数集的以$m$为模的剩余类。

现在来回答第二个问题：分类的依据是什么？比如例 2 中把全班学生按年龄分四类，那么这个分类是依据什么进行的呢？我们知道，在学生中间存在“同龄”（即年龄相同）这个关系，同龄关系在此分类中起着支配作用：有同龄关系的学生都在同一类里；没有同龄关系的学生都在不同的类里；而且每

个学生都与自己有同龄关系．实际上，这个分类是依据同龄关系进行的．

对一般集合所做的每一个分类，也都存在着起支配作用的一种特殊关系．这里我们先对“关系”这个概念做进一步探讨．

“关系”一词，我们早有接触，诸如同学关系，血统关系，同龄关系，实数的大于（$>$）关系，相等（$=$）关系，小于（$<$）关系，整数的整除关系等等．这里需要指出的是，就一个关系来说，它不是在每个集合上都有意义．比如同学关系在整数集上就没有意义，不是整数集上的关系；整数的整除关系在人的集合上也没有意义，不是人与人之间的关系．一般说来

一个关系 R（表示一个关系的记号）是集合 A 上的关系当且仅当对 A 的任二元素 a，b，能够断定 a 对 b 有还是没有关系 R．

当 a 对 b 有关系 R 时，记为 aRb；当 a 对 b 没有关系 R 时，记为 $a\not R b$．于是，就一个集合 A 和一个关系 R 而言，如果 $\forall a, b\in A$ 必有而且只有 aRb 或 $a\not R b$ 之一成立，那么 R 就是 A 上的一个关系．

例 6　对于整数集 Z，大于关系“$>$”，整除关系“$|$”都是 Z 上的关系．因为 $\forall a, b\in Z$，必有而且只有 $a>b$ 或 $a\not> b$ 之一成立．同样，必有而且只有 $a|b$ 或 $a\nmid b$ 之一成立．如果这样规定 R：

$$aRb \Longleftrightarrow ab\geqslant 0 \quad \forall a, b\in Z$$

那么显然 R 是 Z 上的一个关系．有的关系不宜用简短语句描述时，只用记号表示就可以了．

如果这样规定 R'：$\forall a, b\in Z$；当 a，b 同（正负）号，则 $aR'b$；当 a，b 异号，则 $a\not R' b$．那么 R' 就不是 Z 上的关系，因为 0 既不具有正号，也不具有负号，不能说 0 与 0 是同号还是异号，$0R'0$ 与 $0\not R' 0$ 这两者都不成立．

例 7 设m是一个正整数，$\forall a, b \in \mathbf{Z}$，规定

$$aRb \Longleftrightarrow m \mid a-b$$

显然对任二整数a和b，必有$m \mid a-b$或$m \nmid a-b$之一成立，所以R是$\mathbf{Z}$上的一个关系．设以m除a和b所得余数分别为r_1和r_2，易知

$$m \mid a-b \Longleftrightarrow r_1 = r_2$$

事实上，由 $a = mq_1 + r_1$，$b = mq_2 + r_2$，$0 \leqslant r_1, r_2 < m$，得 $a - b = m(q_1 - q_2) + (r_1 - r_2)$，$0 \leqslant |r_1 - r_2| < m$．

当$m \mid a-b$时，有$m \mid r_1 - r_2$，从而$r_1 - r_2 = 0$，故$r_1 = r_2$．反之，当$r_1 = r_2$时，因$r_1 - r_2 = 0$有$a - b = m(q_1 - q_2)$，故$m \mid a-b$．因此$\mathbf{Z}$上的这个关系R叫做以m为模同余（关系）．

是不是每个关系都能用来分类呢？不是，试看例 6 中给出的三个关系．

假如依据大于关系“$>$”对$\mathbf{Z}$做出了分类，那么每个类S中的任二整数之间都应有大于关系．这是做不到的，其实，当$a \in S$，则$a \not> a$，即a与a之间就没有大于关系．

假如依据整除关系“$\mid$”对$\mathbf{Z}$做出了分类，那么对于任意两个不同整数a，b，应该能够明确回答a与b是否同分在一个类里．这是做不到的．比如对于 2 和 4 来说，从$2 \mid 4$来看，它们同在一个类里，但从$4 \nmid 2$看，它们各在不同的类里．所以用整除无法断定 2 和 4 是不是分在同一类里．

假如依据关系R对$\mathbf{Z}$做出了分类．由于 0 与每个整数都有关系R，0 必在每个类中．但是不同的类是不相交的．于是只剩下一种可能：不存在不同的类，即全体整数都在一个类里．这是做不到的：正数与负数之间无关系R，不能同在一个类里．

由上面的分析看出，例 6 中给出的三个关系都不能用来分类．那么什么样的关系可以用来分类呢？下面的讨论告诉我们：等价关系就可以，而且只有等价关系才可以．

定义 2 设$\sim$是A上的一个关系，$\forall a, b, c \in A$，如果满

足下列条件

（1）反身性：$a\sim a$

（2）对称性：若$a\sim b$　则$b\sim a$

（3）传递性：若$a\sim b$，$b\sim c$　则 $a\sim c$

则称$\sim$是A的一个等价关系。

例 6 中给出的$\mathbf{Z}$上的三个关系都不是等价关系。大于关系无反身性和对称性，整除关系无对称性，关系R无传递性。例 7 中的同余是等价关系。

现在我们来指出等价关系与分类之间的相互依存的联系。

定理　集合A的一个等价关系决定A的一个商集；A的一个商集决定A的一个等价关系。

证明　先证定理的第一个结论。设$\sim$是A的一个等价关系，$\forall a\in A$，令

$$\overline{a}=\{x\in A\mid x\sim a\}$$

再令

$$Q=\{\overline{a}\mid a\in A\}$$

下面证明Q是A的一个商集。

（1）$\forall a\in A$，由反身性知$a\in\overline{a}$，从而$a\in\bigcup\limits_{\overline{a}\in Q}\overline{a}$，故$A=\bigcup\limits_{\overline{a}\in Q}\overline{a}$。

（2）$\forall\overline{a}$，$\overline{b}\in Q$，$\overline{a}\neq\overline{b}$，有$\overline{a}\cap\overline{b}=\phi$。否则存在$c\in\overline{a}\cap\overline{b}$，于是$c\sim a$且$c\sim b\Rightarrow a\sim c$且$c\sim b\Rightarrow a\sim b$。由此可推得$\overline{a}=\overline{b}$的矛盾结果。事实上，$\forall x\in\overline{a}$，由$x\sim a$知$x\sim b$，得$x\in\overline{b}$，故有$\overline{a}\subseteq\overline{b}$。反之，$\forall y\in\overline{b}$，由$y\sim b$知$y\sim a$，得$y\in\overline{a}$，故$\overline{a}\supseteq\overline{b}$。所以$\overline{a}=\overline{b}$。

（3）$\forall\overline{a}\in Q$，因$a\sim a$，$a\in\overline{a}$，故$\overline{a}\neq\phi$。

总之，Q满足商集的定义条件，是A的一个商集。Q叫做**由$\sim$决定的商集**。

其次证明定理第二个的结论。设Q是A的一个商集，

$\forall a, b\in A$规定

$$a\sim b\Longleftrightarrow 存在S\in Q使得\ a,\ b\in S$$

由商集的定义知，a，b或者同属于一个类或者分别属于不同的类，二者必居其一．所以，所规定的～是A的一个关系．下面证明～是A的一个等价关系．

（1）由商集定义中的条件1知，$\forall a\in A$，必有$S\in Q$使得$a\in S$，故$a\sim a$．

（2）$\forall a$，$b\in A$，如果$a\sim b$，则存在$S\in Q$使得a，$b\in S$．两个元素同属于一个集合无先后之分，自然有b，$a\in S$，故$b\sim a$．

（3）$\forall a$，b，$c\in A$，如果$a\sim b$，$b\sim c$，则存在S，$T\in Q$使得a，$b\in S$，b，$c\in T$．由$b\in S\cap T$知$S\cap T\neq\phi$，再由商集定义的条件（2）得$S=T$，从而a，$c\in S$，故$a\sim c$．

综上所述，～是A的一个等价关系，～叫做由Q决定的等价关系．证完．

例8　在例7中，对于整数集$\boldsymbol{Z}$和正整数m，给出了一个等价关系R——以m为模同余：$\forall a$，$b\in\boldsymbol{Z}$，

$$aRb\Longleftrightarrow m\mid a-b$$

那么R所决定的$\boldsymbol{Z}$的商集是什么？

解　由上定理的证明知，$\forall a\in\boldsymbol{Z}$，$a$所在的类为

$$\overline{a}=\{x\in\boldsymbol{Z}\mid xRa\}$$

R所决定的商集为

$$Q=\{\overline{a}\mid a\in\boldsymbol{Z}\}$$

用m除a得$a=q'm+r$，$0\leqslant r<m$，$r\in\boldsymbol{Z}$，则$r\in\overline{a}$，于是

$$\overline{a}=\overline{r}=\{x\in\boldsymbol{Z}\mid xRr\}=\{x\in\boldsymbol{Z}\mid x=qm+r,\ q\in\boldsymbol{Z}\}$$

显然$\overline{a}$是以m为模的剩余类：$\overline{a}\in\boldsymbol{Z}_m$（见例5）．反之，$\forall\overline{i}\in\boldsymbol{Z}_m$，显然有$\overline{i}\in Q$．故$Q=\boldsymbol{Z}_m$．即以$m$为模同余所决定的商集正是以$m$为模的剩余类商集$\boldsymbol{Z}_m$．

还可以证明，$\boldsymbol{Z}_m$所决定的等价关系～恰是$\boldsymbol{Z}$的以m为模同余．事实上，由本节定理的证明知，$\forall a$，$b\in\boldsymbol{Z}$，

$$a\sim b\Longleftrightarrow 存在\overline{i}\in\boldsymbol{Z}_m使\ a,\ b\in\overline{i}\Longleftrightarrow m\mid a-b.$$

Z_m与以m为模同余之间的联系具有一般性：设A为任一集合，如果A的等价关系～所决定的商集为Q，那么Q所决定的等价关系恰是～。作为习题，请读者给出其证明。

习　　题

1　$\forall (x, y), (x', y') \in \mathbf{R} \times \mathbf{R}$，令

$(x, y) \sim (x', y') \Longleftrightarrow x - x$ 和$y - y$ 都是整数

证明～是$\mathbf{R} \times \mathbf{R}$的等价关系。

2　证明"="是$\mathbf{R}$的等价关系，并写出它所决定的商集。

3　给出整数集$\mathbf{Z}$的一个恰含四个元素的商集$\mathbf{Q}$，并求出$\mathbf{Q}$所决定的等价关系～。

4　设$A = \{a, b, c, d\}$，试给出A的一个等价关系。

5　对$A = \{a, b, c\}$，给出一个关系～，使～具有对称性、传递性但无反身性。

§4　代数体系

前已指出，近世代数的主要研究对象是代数体系。做为对以后几章研究具体代数体系的准备，本节概括地介绍这一概念。

除集合而外，代数体系的另一组成部分是代数运算。我们先从代数运算讨论起。这个词我们早有接触，如数的四则运算，多项式的加、减、乘运算，矩阵的加、乘运算，数与矩阵的乘法等都是代数运算。现在我们把这个概念推广到一般集合上去。

定义1　设A，B，C是三个非空集合，则$A \times B$到C的任一映射$\circ$叫做A与B到C的一个代数运算，简称为运算。当$A = B = C$时，则A与A到A的运算叫做A的运算*。

设"$\circ$"是A与B到C的运算，$\forall (a,b) \in A \times B$：如果$(a, b)$

* 当$\circ$是A的运算时，有时也说A对于$\circ$封闭。

在“$\circ$”之下的象是$c\in C$，依照映射记法，本应写作$\circ((a,b))=c$。但为了适应通常的习惯，改成$a\circ b=c$。

例 1　设C是复数集，$\forall a,\ b\in C$ 规定

$$\circ_1:\ (a,\ b)\longmapsto a+b$$

$$\circ_2:\ (a,\ b)\longleftarrow\!\!\dashv a\cdot b$$

因为$\circ_1$和$\circ_2$都是$C\times C$到C的映射，所以$\circ_1$和$\circ_2$都是C的运算。按约定写法应记作

$$a\circ_1 b=a+b$$

$$a\circ_2 a=a\cdot b$$

上面所定义的两个运算$\circ_1$和$\circ_2$恰是复数的加法和乘法，即通常的加法和乘法都是C的代数运算。

例 2　设F是一个数域，$V(F)$ 是F上的线性空间，用类似例 1 的讨论方法可以看出：向量加法是 $V(F)$ 的运算，数乘向量的乘法是F与 $V(F)$到$V(F)$的运算。

例 3　$\forall a,\ b\in R$，规定

$$a\circ_1 b=\max[a,\ b]$$

$$a\circ_2 b=\min[a,\ b]$$

因为$\circ_1$和$\circ_2$都是 $R\times R$ 到R的映射，所以都是R的运算。即对任二实数取最大数和取最小数都是实数集R的运算。

例 4　设A是任一集合，$\forall S,\ T\in P(A)$，规定

$$S\circ_1 T=S\cup T$$

$$S\circ_2 T=S\cap T$$

因$\circ_1$和$\circ_2$都是 $P(A)\times P(A)$ 到 $P(A)$的映射，故都是幂集$P(A)$ 的运算。即对一个集合的任二子集取并或取交都是该集合的幂集的运算。

例 5　设A是任一非空集合，$T(A)$ 是A的所有变换的集合，$\forall\psi,\ \varphi\in T(A)$，规定

$$\psi\circ\varphi=\psi\varphi$$

在§2里已经指出，A的任二变换的合成仍然是A的一个变换，所以“$\circ$”是$T(A)\times T(A)$到$T(A)$的映射，是$T(A)$的一个运

算．这个运算叫做变换乘法，而变换 $\psi\varphi$ 叫做 ψ 与 φ 的乘积．我们看到，变换乘法是由变换合成确定的，ψ 与 φ 的乘积正是 φ 与 ψ 的合成．

例 6　设 $A=\{1, 2, \cdots, n\}$ 是 n 元有限集合，S_n 是 A 的所有置换集合．每个置换都是 A 的变换，例 5 已给出变换乘法，所以对于 S_n 中的任二元素（n 元置换）ψ，φ 可以求它们的变换乘积 $\psi\varphi$．这是置换 φ 与置换 ψ 的合成，§2已指出两个 n 元置换的合成仍然是 n 元置换，所以 $\psi\varphi\in S_n$．这说明 S_n 对于变换乘法封闭，变换乘法是 S_n 的运算．S_n 的这个运算也叫做置换乘法．

§2里已经给出表示置换的记号，以及求该记号所表示两个置换合成的方法．为了便于运算，这里对置换再给出一种表示法，将置换表成轮换之积．

首先说明，什么是轮换．设 φ 是 $A=\{1, 2, \cdots, n\}$ 的一个置换，如果 φ 循环地变换 $r>1$ 个不同数码 $i_1, i_2, \cdots, i_r$，即 φ：$i_1\longmapsto i_2$，$i_2\longmapsto i_3$，$\cdots$，$i_{r-1}\longmapsto i_r$，$i_r\longmapsto i_1$，而且 A 中其余的 $n-r$ 个数码在 φ 之下不变，此时 φ 叫做 r 阶轮换，记为

$$\varphi=(i_1i_2\cdots i_r)$$

也可以记为

$$\varphi=(i_2i_3\cdots i_ri_1)=(i_3i_4\cdots i_1i_2)=\cdots$$

这个记法表示：不在括号中出现的数码，在 φ 之下不变；在括号中出现的数码，在 φ 之下的象列在它相邻右侧，括号中右端数码的象列在左端．例如

$$\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}=(1\ 2\ 3)=(2\ 3\ 1)=(3\ 1\ 2)$$

$$\begin{pmatrix}1&2&3&4&5\\1&5&2&4&3\end{pmatrix}=(2\ 5\ 3)=(5\ 3\ 2)=(3\ 2\ 5)$$

我们规定，A 的恒等置换 I_A 记为

$$I_A=\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix}=(1)=(2)=\cdots=(n)$$

叫做1阶轮换。如果两个轮换 $\varphi=(i_1i_2\cdots i_r)$，$\psi=(j_1j_2\cdots j_s)$在它们的轮换记号中无相同数码，则说 φ 与 ψ 不相交。

容易看出，存在着不是轮换的置换。例如

$$\varphi=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 5 & 4\end{pmatrix}$$

就不是轮换。事实上，此置换使$\varphi(i)\neq i$，$i=1$，2，3，4，5。这说明，如果 φ 是轮换，它一定是5阶轮换。但是φ：$1\longmapsto 2$，$2\longmapsto 3$，$3\longmapsto 1$，可见 φ 不能是5阶轮换。实际上，由置换乘法，$\varphi=(1\ 2\ 3)(4\ 5)$ 。一般来讲：

每个置换都可表成不相交轮换之积。

限于篇幅，此命题的证明从略。

例如

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 1 & 5 & 2 & 3\end{pmatrix}=(1\ 4\ 2)(3\ 5)$$

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 5 & 4 & 6 & 2 & 1 & 3 & 7\end{pmatrix}=(1\ 5)(2\ 4)(3\ 6)$$

请读者按置换的新表示法练习求置换的乘积。假设φ，$\psi\in S_5$，$\varphi=(1\ 2\ 3)(4\ 5)$，$\psi=(1\ 4\ 2)(3\ 5)$，则

$$\begin{aligned}\varphi\psi&=[(1\ 2\ 3)(4\ 5)][(1\ 4\ 2)(3\ 5)]\\&=(1\ 5)(3\ 4)\end{aligned}$$

例7　对于以m为模剩余类商集 $Z_m=\{\overline{0},\overline{1},\cdots,\overline{m-1}\}$，由§3例8容易推得，$\forall k$，$h\in Z$ 有

$$\overline{k}=\overline{h}\Longleftrightarrow m\mid k-h \tag{1}$$

（注意：此处k，h 不必小于m，$\overline{k}$表示k所在的类，比如$m+1\in\overline{1}$，则$\overline{m+1}=\overline{1}$。）现在对集合 Z_m定义称为剩余类加法和剩余类乘法的运算，仍然分别采用记号“+”和“·”

（在运算过程中，乘号也可略去不写）。$\forall \bar{k}, \bar{h} \in Z_m$，规定：

$$+: \bar{k} + \bar{h} = \overline{k+h} \quad (2)$$

$$\cdot: \bar{k} \cdot \bar{h} = \overline{k \cdot h} \quad (3)$$

上两式等号右端的"+"和"·"是通常数的加法和乘法。

现在来说明上述两个法则都是 Z_m 的代数运算。对于元素（类）$\bar{k}$ 和 $\bar{h}$ 来说，元素 $\overline{k+h}$ 和 $\overline{k \cdot h}$ 显然是 Z_m 中的元素。另一方面，我们注意，Z_m 中的元素（类）是用该类所含的任一整数来表示的，同一个元素（类）的表法并不唯一。如整数 k 和 k' 同在一个类，那么 k 和 k' 都可做为这个类的代表：$\bar{k} = \overline{k'}$，这就产生一个问题：法则（2）和（3）都是用代表描述的，对同样元素是否会因取不同的代表而得到不同的结果？因此，要说明（2）和（3）所定义的+和·是代数运算，必须说明 $\overline{k+h}$ 和 $\overline{k \cdot h}$ 与代表的选取无关，是唯一确定的。

设 $\overline{k'} = \bar{k}$，$\overline{h'} = \bar{h}$。由（1）知

$$m \mid k' - k, \quad m \mid h' - h$$

于是整数

$$(k' + h') - (k + h) = (k' - k) + (h' - h)$$

可被 m 整除，再由（1）得

$$\overline{k' + h'} = \overline{k + h}$$

这说明对于 $\bar{k}$ 和 $\bar{h}$ 来说（无论选取哪个代表），元素 $\overline{k+h}$ 是唯一确定的。

同理，整数

$$k'h' - kh = k'(h' - h) + h(k' - k)$$

可被 m 整除，故

$$\overline{k'h'} = \overline{kh}$$

即 $\overline{kh}$ 也与代表的选取无关，是唯一确定的。

综上所述，由（2）、（3）规定的剩余类加法和剩余类乘法都是 Z_m 的代数运算。

当 A 是有限集合时，A 的运算"∘"可用一个表去表示。如

$A=\{a_1,\ a_2,\ \cdots,\ a_i,\ \cdots,\ a_j,\ \cdots,\ a_n\}$，则表

$\circ$	a_1	$\cdots$	a_i	$\cdots$	a_j	$\cdots$	a_n
a_1	$a_1\circ a_1$	$\cdots$	$a_1\circ a_i$	$\cdots$	$a_1\circ a_j$	$\cdots$	$a_1\circ a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$		$\vdots$
a_i	$a_i\circ a_1$	$\cdots$	$a_i\circ a_i$	$\cdots$	$a_i\circ a_j$	$\cdots$	$a_i\circ a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$		$\vdots$
a_j	$a_j\circ a_1$	$\cdots$	$a_j\circ a_i$	$\cdots$	$a_j\circ a_j$	$\cdots$	$a_j\circ a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$		$\vdots$
a_n	$a_n\circ a_1$	$\cdots$	$a_n\circ a_i$	$\cdots$	$a_n\circ a_j$	$\cdots$	$a_n\circ a_n$

（4）

叫做“$\circ$”的运算表（当运算叫做加法或乘法时，此表便叫做加法表或乘法表）。表（4）中第 i 行第 j 列位置的元素是 $a_i\circ a_j$，这样，表（4）便列出了A的任意两个元素的运算结果。

对有限集合的任一运算，都可造出一个运算表，反之，任意一个形如（4）的表，也都确定有限集合的一个运算。运算表的好处是，运算结果一目了然，它能显示出该运算的许多性质，而且对有限集合有时也可从造出形如（4）的表入手来定义运算。

例 8　$Z_3=\{\overline{0},\ \overline{1},\ \overline{2}\}$ 的（剩余类）加法表和乘法表为

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

设S_3：$\varphi_1=(1)$，$\varphi_2=(12)$，$\varphi_3=(13)$，$\varphi_4=(23)$，$\varphi_5(123)$，$\varphi_6=(132)$。S_3 的（置换）乘法表为

·	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_1	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_2	φ_2	φ_4	φ_6	φ_1	φ_5	φ_3
φ_3	φ_3	φ_5	φ_1	φ_6	φ_2	φ_4
φ_4	φ_4	φ_6	φ_5	φ_1	φ_3	φ_2
φ_5	φ_5	φ_3	φ_4	φ_2	φ_6	φ_1
φ_6	φ_6	φ_4	φ_2	φ_3	φ_1	φ_5

现在来讨论代数体系概念。

定义 2　对于给定的非空集合（可不只一个）定义了代数运算（可不只一个）便确定一个代数体系，它是由给定的集合与所定义的代数运算组成的共同体。

例 9　设 V 是数域 F 上的线性空间。这里有两个集合：F 和 V，还有四个运算：数的加法和乘法，数乘向量的乘法和向量加法。F 和 V 与这四个代数运算共同组成一个代数体系。

设 C 是复数集，数的加法“+”和乘法“·”是 C 的代数运算，于是 C 与 +，· 共同组成一个代数体系。自然 C 与 +，C 与 · 也各组成一个代数体系。

设 S_n 是 n 元置换集合，“·”是置换乘法，则 S_n 与 · 组成一个代数体系。

以后我们所讨论的多是由一个集合与几个代数运算所组成的代数体系，特对这类代数体系给出表示记号。设 $\circ_1$，$\circ_2$，…，$\circ_n$ 是集合 A 的 n 个代数运算，则由 A 和这 n 个运算组成的代数体系记为 $\{A;\ \circ_1,\ \circ_2,\ \cdots \circ_n\}$。我们最常见的是 $n=1$ 和 $n=2$ 的情形。

例10　现把在后几章将多次遇到的代数体系列举如下

$\{N;+,\ \cdot\}$，$\{N;+\}$，$\{N;\cdot\}$

$\{Z;+,\ \cdot\}$，$\{Z;+\}$，$\{Z;\cdot\}$，$\{\dot{Z};\cdot\}$

$\{Q;+,\ \cdot\}$，$\{Q;+\}$，$\{Q;\cdot\}$，$\{\dot{Q};\cdot\}$

$\{R;+,\ \cdot\}$，$\{R;+\}$，$\{R;\cdot\}$，$\{\dot{R};\cdot\}$

$\{C;+,\ \cdot\}$，$\{C;+\}$，$\{C;\cdot\}$，$\{\dot{C};\cdot\}$

其中"+"和"·"分别是数的加法和乘法；$\dot{Z}$，$\dot{Q}$，$\dot{R}$，$\dot{C}$分别表示所有非零整数集，所有非零有理数集，所有非零实数集，所有非零复数集。

$\{Z_m;+\ \cdot\}$，$\{Z_m;+\}$，$\{Z_m;\cdot\}$

其中"+"和"·"分别是剩余类加法和乘法。

$\{T(A);\ \cdot\}$，$\{S_n;\cdot\}$

其中"·"是变换乘法，$T(A)$ 表示集合A的所有变换的集合。

$\{M_n(F);\ +,\ \cdot\}$，$\{M_n(F);+\}$，$\{M_n(F);\ \cdot\}$

其中 $M_n(F)$ 表示数域F上的全体n阶方阵集合，"+"和"·"分别是矩阵加法和乘法。

$\{F[x];\ +,\ \cdot\}$，$\{F[x];\ +\}$，$\{F[x];\ \cdot\}$

其中$F[x]$表示数域F上的所有多项式集合，"+"和"·"分别是多项式加法和乘法。

定义 3　由一个非空集合A和A的一个代数运算"∘"组成的代数体系$\{A;\ \circ\}$叫做广群。

例10列举的代数体系中，大多数是广群。那些广群具有一个共同特点：运算满足结合律．不满足结合律的广群是存在的，如$\{Z;\ -\}$，$\{\dot{Q};\ \div\}$便是。

为了叙述方便，有时把广群$\{A;\ \circ\}$的运算"∘"叫做乘法，并用乘号"·"代替"∘"，在做运算时常把乘号"·"略去不写．也有时把运算"∘"叫做加法，并用"+"代替"∘"．还有时为了简便，只用集合A来代表广群$\{A;\ \circ\}$，而把A叫做广群。此时我们应该意识到存在着A的一个运算。

定义 4　设S是广群A的子集，如果S关于A的运算也构成广群，则S叫做A的子广群。

例如，在广群$\{C;\ +\}$，$\{R;\ -\}$，$\{Q;\ +\}$，$\{Z;\ +\}$，

$\{N;+\}$中，后者都是前者的子广群．任一广群A都是其自身的子广群．

这里需注意，子广群定义中，S的运算必须与A的运算相同，S才是A的子广群．例如，$\mathbf{R}$是$\mathbf{C}$的子集，但$\{\mathbf{R};\cdot\}$不是$\{\mathbf{C};+\}$的子广群，尽管$\{\mathbf{R};\cdot\}$是一个广群．

习　　题

1　设$A=\{a, b, c, d\}$，试对A定义两个不同的代数运算$\circ_1$，$\circ_2$，使$\{A;\circ_1,\circ_2\}$是代数体系．

2　列举S_4的全部元素（表成轮换之积）．S_4的子集$A=\{(1), (1234), (13)(24), (1432)\}$关于置换乘法是$S_4$的子广群，试制出$A$的乘法表．

3　试制出$\mathbf{Z}_5$的（剩余类）加法表和乘法表．

§5　同态　同构

我们已经知道，两个集合可以通过映射建立联系，那么两个代数体系之间是否也可以通过映射建立联系呢？由于代数体系具有集合部分，所以这样做是完全可以的．但是，与两个代数体系的运算无关的映射，所起的联系作用有着很大的局限性．本节将讨论两类与运算密切相关的映射，这两类映射在代数学的研究中起着重要的作用．

以最简单的情况为例．设$\{A;\circ\}$和$\{B;\circ'\}$是两个广群，φ是A到B的一个映射．$\forall a, b\in A$，它们在φ之下的象是$\varphi(a)$，$\varphi(b)\in B$．a与b做运算$\circ$的结果是元素$a\circ b\in A$，$\varphi(a)$与$\varphi(b)$做运算$\circ'$的结果是元素$\varphi(a)\circ'\varphi(b)$．在一般情况下，元素$a\circ b$在$\varphi$之下的象不一定是元素$\varphi(a)\circ'\varphi(b)$．如果$\varphi$是一个特殊的映射，它能保证$a\circ b$的象是$\varphi(a)\circ'\varphi(b)$，那么$\varphi$不仅对集合$A$与集合$B$，而且对运算$\circ$和$\circ'$，从而对广群$\{A;\circ\}$和$\{B;\circ'\}$起着联系作用．

定义 1 设$\{A;\circ\}$和$\{B;\circ'\}$是两个代数体系，如果映射φ: $A\to B$使得$\forall a,b\in A$有

$$\varphi:\ a\circ b\longmapsto\varphi(a)\circ'\varphi(b)$$

即

$$\varphi(a\circ b)=\varphi(a)\circ'\varphi(b)$$

则φ叫做$\{A;\circ\}$到$\{B;\circ'\}$的一个同态映射，简称同态。

例 1 设$\{A;\circ\}$是任一广群，$\{Z;\ \cdot\}$是整数乘法广群，考虑A到Z的映射

$$\varphi:\ a\longmapsto 1,\quad \forall a\in A$$

因为 $\forall a,\ b\in A$有

$$\varphi(a\circ b)=1,\quad \varphi(a)\cdot\varphi(b)=1$$

故

$$\varphi(a\circ b)=\varphi(a)\cdot\varphi(b)$$

所以φ是$\{A;\ \circ\}$到$\{Z;\ \cdot\}$的一个同态映射。

例 2 对于$\{Z;\ +\}$考虑映射

$$\varphi:\ n\longmapsto 2n,\quad \forall n\in Z$$

因$\forall n,\ m\in Z$，有

$$\varphi(n+m)=2(n+m)=2n+2m=\varphi(n)+\varphi(m)$$

故φ是$\{Z;\ +\}$到$\{Z;\ +\}$的一个同态映射，但φ不是$\{Z;\ \cdot\}$到$\{Z;\ \cdot\}$的同态映射，因为不能保证

$$\varphi(n\cdot m)=\varphi(n)\cdot\varphi(m)$$

比如当 $n=1$，$m=3$ 时，

$$\varphi(1\times 3)=\varphi(3)=6$$

但是

$$\varphi(1)\cdot\varphi(3)=2\times 6=12$$

定义 2 设φ是$\{A;\ \circ\}$到$\{B;\ \circ'\}$的同态映射，如果φ是A到B的单射、满射或双射，则φ分别叫做$\{A;\ \circ\}$到$\{B;\ \circ'\}$的单一同态、满同态或同构。当φ是满同态时，也说$\{A;\ \circ\}$与$\{B;\ \circ'\}$在φ之下同态，记为φ: $\{A;\ \circ\}\sim\{B;\ \circ'\}$或$\{A;\ \circ\}\overset{\varphi}{\sim}\{B;\ \circ'\}$。当$\varphi$是同构时，也说$\{A;\ \circ\}$与$\{B;\ \circ'\}$在$\varphi$之下同

构，记为 φ：$\{A;\ \circ\}\cong\{B;\ \circ'\}$或$\{A;\ \circ\}\cong\{B;\ \circ'\}$。

例　对于$\{Z;\ +\}$与$\{Z_m;\ +\}$，以及$\{Z;\ \cdot\}$与$\{Z_m;\ \cdot\}$，考虑Z到Z_m的映射

$$\varphi:\ a\longmapsto\overline{a},\quad \forall a\in Z$$

显然φ是满射，而且φ保持运算：$\forall a,\ b\in Z$ 有

$$\varphi(a+b)=\overline{a+b}=\overline{a}+\overline{b}=\varphi(a)+\varphi(b)$$

$$\varphi(a\cdot b)=\overline{a\cdot b}=\overline{a}\cdot\overline{b}=\varphi(a)\cdot\varphi(b)$$

故

$$\varphi:\ \{Z;\ +\}\sim\{Z_m;\ +\}$$

$$\varphi:\ \{Z;\ \cdot\}\sim\{Z_m;\ \cdot\}$$

例 4　设 $B=\{1,\ -1\}$，B 关于数的乘法构成广群。对于$\{Z_2;+\}$与$\{B;\ \cdot\}$考虑映射

$$\varphi:\ \overline{0}\longmapsto 1,\qquad \overline{1}\longmapsto -1$$

显然φ是双射，而且可以证明，$\forall a,\ b\in Z_2$，

$$\varphi(a+b)=\varphi(a)\cdot\varphi(b)$$

事实上，当a，b中有$\overline{0}$时，不失一般性可令$a=\overline{0}$，此时 $\varphi(a)=1$，则

$$\varphi(a+b)=\varphi(\overline{0}+b)=\varphi(b)=1\cdot\varphi(b)=\varphi(a)\cdot\varphi(b)$$

当 $a=b=\overline{1}$ 时，$\varphi(a)=\varphi(b)=-1$。则

$$\varphi(a+b)=\varphi(\overline{1}+\overline{1})=\varphi(\overline{0})=1=(-1)\cdot(-1)$$
$$=\varphi(a)\cdot\varphi(b)$$

故

$$\varphi:\ \{Z_2;\ +\}\cong\{B;\ \cdot\}$$

同态、同构概念可推广到具有 n 个代数运算的代数体系上去。

定义 3　设$\{A;\ \circ_1,\ \circ_2,\ \cdots,\ \circ_n\}$和$\{B,\ \circ'_1,\ \circ'_2,\ \cdots,\ \circ'_n\}$是两个代数体系，如果映射$\varphi$：$A\longrightarrow B$使得$\forall a,\ b\in A$ 有

$$\varphi:\ a\circ_i b\longmapsto\varphi(a)\circ'_i\varphi(b)$$

即

$$\varphi(a\circ_i b)=\varphi(a)\circ'_i\varphi(b),\quad i=1,\ 2,\ \cdots,\ n$$

则φ叫做$\{A; \circ_1, \circ_2, \cdots, \circ_n\}$到$\{B; \circ'_1, \circ'_2, \cdots, \circ'_n\}$的同态映射，简称同态．当$\varphi$是单射、满射或双射时，$\varphi$分别叫做单一同态、满同态或同构．对后两种情况，相应地有与定义2后部分相类似的规定和记号．

例如由例3知

$$\varphi: \{Z; +, \cdot\} \sim \{Z_n; +, \cdot\}$$

在后面的讨论中将看到：两个同态的代数体系有许多相同之处，可以通过其中之一所具有的性质去估计另一个的性质．两个同构的代数体系，则具有完全相同的代数性质．此时，从代数观点看，它们没有任何差别，是等同的．

命题1 **设φ和ψ分别是$\{A; \circ_1, \circ_2, \cdots, \circ_n\}$到$\{B; \circ'_1, \circ'_2, \cdots \circ'_n\}$和$\{B; \circ'_1, \circ'_2, \cdots, \circ'_n\}$到$\{C; \circ''_1, \circ''_2, \cdots, \circ''_n\}$的同态映射，则$\psi\varphi$是$\{A; \circ_1, \circ_2, \cdots, \circ_n\}$到$\{C; \circ''_1, \circ''_2, \cdots, \circ''_n\}$的同态映射．如果$\varphi$和$\psi$都是单一同态、满同态或同构，那么$\psi\varphi$也必是单一同态、满同态或同构．**

证明 由§2知，当φ和ψ都是单射、满射或双射时，$\psi\varphi$必是单射、满射或双射．这里只须证明$\psi\varphi$保持运算．事实上，$\forall a, b \in A$有

$$\begin{aligned}\psi\varphi(a\circ_i b) &= \psi(\varphi(a\circ_i b)) = \psi(\varphi(a)\circ'_i\varphi(b)) \\ &= \psi(\varphi(a))\circ''_i\psi(\varphi(b)) \\ &= \psi\varphi(a)\circ''_i\psi\varphi(b), \quad i = 1, 2, \cdots, n\end{aligned}$$

证完．

命题2 **设$\{A; \circ_1, \circ_2, \cdots, \circ_n\} \overset{\varphi}{\cong} \{B; \circ'_1, \circ'_2, \cdots, \circ'_n\}$，则$\{B; \circ'_1, \circ'_2, \cdots, \circ'_n\} \overset{\varphi^{-1}}{\cong} \{A; \circ_1, \circ_2, \cdots, \circ_n\}$．**

证明 由同构的定义知φ是双射，再由§2知，φ^{-1}是B到A的双射．另外，$\forall a', b' \in B$，设$\varphi^{-1}(a') = a$，$\varphi^{-1}(b') = b$，则$\varphi(a) = a'$，$\varphi(b) = b'$．于是

$$\varphi^{-1}(a'\circ'_i b') = \varphi^{-1}(\varphi(a)\circ'_i\varphi(b)) = \varphi^{-1}(\varphi(a\circ_i b))$$

$$=\varphi^{-1}\varphi(a\circ_i b)=a\circ_i b$$
$$=\varphi^{-1}(a')\circ_i\varphi^{-1}(b')$$

故

$$\{B;\ \circ'_1,\ \circ'_2,\ \cdots,\ \circ'_n\}\cong\{A;\ \circ_1,\ \circ_2,\ \cdots,\ \circ_n\}$$

证完。

定义 3 设$\{A;\ \circ_1,\ \circ_2,\ \cdots,\circ_n\}$是一个代数体系，则$\{A;\ \circ_1,\ \circ_2,\ \cdots,\ \circ_n\}$ 到其自身的同态映射叫做此代数体系的自同态。$\{A;\ \circ_1,\ \circ_2,\ \cdots,\ \circ_n\}$ 到其自身的同构映射叫做此代数体系的自同构。

由命题 1 可以推得：$\{A;\ \circ_1,\ \circ_2,\ \cdots,\ \circ_n\}$ 的任意两个自同态的乘积（变换乘法）仍然是它的自同态；$\{A;\ \circ_1,\ \circ_2,\cdots,\ \circ_n\}$的任意两个自同构的乘积，仍然是它的自同构。所以$\{A;\ \circ_1,\ \circ_2,\ \cdots,\ \circ_n\}$ 的所有自同态的集合以及它的所有自同构集合，关于变换乘法各组成一个代数体系。

习　　题

1　证明：$\{\mathbf{Z};\ \cdot\}\sim\{\{-1,\ 0,\ 1\};\ \cdot\}$，其中“$\cdot$”是数的乘法。

2　设$A=\{1,\ i,\ -1,\ -i\}$，$B=\{1,\ -1\}$证明

$\{A;\ \cdot\}\sim\{B;\ \cdot\}$

其中“$\cdot$”是数的乘法。

3　设F是一个数域，$V_4=\{(a_1,\ a_2,\ a_3,\ a_4)\mid a_i\in F\}$，$M_2(F)=\left\{\begin{pmatrix}a_1 & a_2\\ a_3 & a_4\end{pmatrix}\mid a_i\in F\right\}$，证明

$$\{V_4;\ +\}\cong\{M_2(F);\ +\}$$

其中同构记号左、右端中的“$+$”分别是向量加法和矩阵加法。

4　找出$\{\mathbf{Z}_3;\ +\}$的所有的自同构。

§6　半群　亚群

为了便于对群、环、模、域的讨论，本节先简单介绍条件

较它们为弱的两类代数体系。

定义1 设$\{A;\ \cdot\}$是广群，如果其乘法“·”满足结合律

$$(a\cdot b)\cdot c=a\cdot(b\cdot c),\quad \forall a,b,c\in A$$

则$\{A;\ \cdot\}$叫做半群，简称A为半群。

§4例10中具有一个运算的代数体系都是半群。

定义2 设$\{A;\ \cdot\}$是半群，S是A的非空子集。如果S关于A的乘法“·”也构成半群，则$\{S;\ \cdot\}$称为$\{A;\ \cdot\}$的子半群。当S是A的真子集时，则$\{S;\ \cdot\}$叫做$\{A;\ \cdot\}$的真子半群。

广群A的子集S关于A的运算构成半群时，也把S叫做广群A的子半群。

§4例10中有许多子半群的例子，读者可自行查阅。

设A是半群，S是A的任一子集。A的乘法在对A的元素进行运算时满足结合律，自然对S的元素进行运算也满足结合律*，所以只要S是A的子广群，S就是A的子半群。因此

半群A的子集S是A的子半群必要而且只要$\forall a,b\in S$，有$a,b\in S$，其中“·”是A的乘法。

结合律表明，在半群A的三个元素a,b,c做运算时，只要它们的前后顺序排定，先从哪两个算起都一样。亦即，当a,b,c的排列顺序确定以后，按任何运算顺序做乘法，其积不变。

$$(a\cdot b)\cdot c=a\cdot(b\cdot c)$$

那么，在更多个元素参加运算时，是否还有这个性质呢？比如四个元素a,b,c,d参加运算，在排列顺序不变的情况下（此时是按字母顺序排列的），有下列五种运算顺序

$$a\cdot(b\cdot(c\cdot d)),\quad (a\cdot b)\cdot(c\cdot d),\quad ((a\cdot b)\cdot c)\cdot d$$

$$a\cdot((b\cdot c)\cdot d),\quad (a\cdot(b\cdot c))\cdot d$$

---

* 一个规律，如果在集合A上成立必然导致在A的每个子集上也成立，则常说此规律具有遗传性，结合律便具有遗传性。

这五个乘积都相等吗？对此有

定理 1　设 $\{A;\ \cdot\}$ 是半群，则“·”满足广义结合律：对于 A 的任意 $n(\geqslant 3)$ 个元素 $a_1,a_2,\cdots,a_n$，在元素排列顺序确定后，按任何一种运算顺序做乘法，所得乘积都相等。

证明　首先规定一个记号。设 $b_1,b_2,\cdots,b_m\in A$，如果这 m 个元素按下标自然顺序排定后，用各种运算顺序乘得的积都相同，则以 $b_1\cdot b_2\cdot\cdots\cdot b_m$ 表示该乘积。

假设 $a_1,a_2,\cdots,a_n$ 按下标自然顺序排列，任取一种运算顺序所乘得的积为 c，只须证明：

$$c=(\cdots((a_1\cdot a_2)\cdot a_3)\cdots)\cdot a_n \tag{1}$$

就元素个数 n 用第二数学归纳法。

当 $n=3$ 时，由结合律知（1）成立。

假设元素个数 $<n$ 时，（1）成立。我们注意，在运算过程中，无论采用的是哪种运算顺序，最后一个步骤一定是

$$d_1\cdot d_2=c$$

其中 d_1 是 $a_1,a_2,\cdots,a_i$ 在下标自然排列顺序下的一个乘积，d_2 是 $a_{i+1},a_{i+2},\cdots,a_n$ 在下标自然排列顺序下的一个乘积，这里 $1\leqslant i<n$。由归纳假设知

$$d_1=a_1\cdot a_2\cdot\cdots\cdot a_i$$

$$d_2={}_{i+1}\cdot a_{i+2}\cdot\cdots\cdot a_n=(a_{i+1}\cdot a_{i+2}\cdot\cdots\cdot a_{n-1})\cdot a_n$$

再由结合律和归纳假设得

$$c=d_1\cdot d_2=(a_1\cdot a_2\cdot\cdots\cdot a_i)\cdot((a_{i+1}\cdot a_{i+2}\cdot\cdots\cdot a_{n-1})\cdot a_n)$$

$$=((a_1\cdot a_2\cdot\cdots\cdot a_i)(a_{i+1}\cdot a_{i+2}\cdot\cdots\cdot a_{n-1}))\cdot a_n$$

$$(\cdots((a_1\cdot a_2)\cdot a_3)\cdots)\cdot a_n$$

故（1）成立。证完。

由定理 1 知，在半群 A 中记号

$$a_1\cdot a_2\cdot\cdots\cdot a_n,\quad a_i\in A$$

是有意义的，它是元素 $a_1,a_2,\cdots,a_n$ 在此排列顺序下的唯一乘积。

定义 3　设 $\{A;\ \cdot\}$ 是半群，如果“·”满足交换律

$$a\cdot b=b\cdot a,\quad \forall a,b\in A$$

则$\{A;\ \cdot\}$叫做交换半群。

例如，数的集合关于数的加法或乘法所做成的半群都是交换半群，$\{Z_m;\ +\}$，$\{Z_n;\ \cdot\}$也都是交换半群。但$\{S_n;\ \cdot\}$ $(n>2)$，$\{M_n(F);\ \cdot\}(n>1)$都是非交换半群。

定理 2 如果$\{A;\ \cdot\}$是交换半群，则"$\cdot$"满足广义交换律：A的任意n个元素$a_1,a_2,\cdots,a_n$按任何一个排列顺序所做得的乘积都相等。

证明 设$i_1i_2\cdots i_n$是$1,2,\cdots,n$的任一排列，只须证明

$$a_{i_1}\cdot a_{i_2}\cdot\cdots\cdot a_{i_n}=a_1\cdot a_2\cdot\cdots\cdot a_n \tag{1}$$

就元素个数n用数学归纳法。

当$n=2$时，由于A的乘法满足交换律，（1）式成立。

假设（1）式对$n-1$成立。在$i_1,i_2,\cdots,i_n$中，必有一个$i_k=n$，则由结合律、交换律和归纳假设得

$$\begin{aligned}
&a_{i_1}\cdot\cdots\cdot a_{i_{k-1}}\cdot a_{i_k}\cdot a_{i_{k+1}}\cdot\cdots\cdot a_{i_n}\\
&=a_{i_1}\cdot\cdots\cdot a_{i_{k-1}}\cdot a_n\cdot a_{i_{k+1}}\cdot\cdots\cdot a_{i_n}\\
&=(a_{i_1}\cdot\cdots\cdot a_{i_{k-1}})\cdot(a_n\cdot(a_{i_{k+1}}\cdot\cdots\cdot a_{i_n}))\\
&=(a_{i_1}\cdot\cdots\cdot a_{i_{k-1}})\cdot((a_{i_{k+1}}\cdot\cdots\cdot a_{i_n})\cdot a_n)\\
&=((a_{i_1}\cdot\cdots\cdot a_{i_{k-1}})\cdot(a_{i_{k+1}}\cdot\cdots\cdot a_{i_n}))\cdot a_n\\
&=(a_1\cdot a_2\cdot\cdots\cdot a_{n-1})\cdot a_n=a_1\cdot a_2\cdot\cdots\cdot a_n
\end{aligned}$$

故（1）成立。证完。

下面来探讨一下同态、同构在半群理论中的作用。

定理 3 设$\{A;\ \circ\}\overset{\varphi}{\sim}\{B;\ \circ'\}$，则当$A$是半群时，$B$必是半群；当$A$是交换半群时，$B$必是交换半群。

证明 设A是半群，我们来证明"$\circ'$"满足结合律。$\forall a',b',c'\in B$，因φ是满射，故存在$a,b,c\in A$，使得$\varphi(a)=a'$，$\varphi(b)=b'$，$\varphi(c)=c'$。再因φ保持运算和"$\circ$"满足结合

律得

$$\begin{aligned}(a'\circ' b')\circ' c' &= (\varphi(a)\circ'\varphi(b))\circ'\varphi(c)\\ &=\varphi(a\circ b)\circ'\varphi(c)\\ &=\varphi((a\circ b)\circ c)\\ &=\varphi(a\circ(b\circ c))\\ &=\varphi(a)\circ'\varphi(b\circ c)\\ &=\varphi(a)\circ'(\varphi(b)\circ'\varphi(c))\\ &=a'\circ'(b'\circ' c')\end{aligned}$$

故$\{B;\ \circ'\}$是半群。

当A是交换半群时，有

$$\begin{aligned}a'\circ' b' &=\varphi(a)\circ'\varphi(b)=\varphi(a\circ b)=\varphi(b\circ a)\\ &=\varphi(b)\circ'\varphi(a)=b'\circ' a'\end{aligned}$$

即"$\circ'$"满足交换律，B是交换半群。证完。

定理 3 说明，满同态保持结合律、交换律；半群的同态象是半群，交换半群的同态象是交换半群。请注意，这个定理的逆命题不真，例如 $\{Z;\ -\}\sim\{\{0\};\ +\}$，后者是交换半群，但前者不是半群。然而对于同构映射有如下

推论 设$\{A;\ \circ\}\cong\{B;\ \circ'\}$，则$A$是半群$\Longleftrightarrow B$是半群，$A$是交换半群$\Longleftrightarrow B$是交换半群。

此推论可由定理 3 和§5命题 2 直接证得。

最后来讨论一类比半群条件再强一点的代数体系。先给出恒等元概念。

定义 4 设A是广群，如果$e\in A$，$\forall a\in A$ 使得

$$ea=a$$

则e叫做A的左恒等元。如果 $e'\in A$，$\forall a\in A$ 使得

$$ae'=a$$

则e'叫做A的右恒等元。如果e既是A的左恒等元，又是A的右恒等元，则e叫做A的恒等元。

由定义可直接推得：广群A如果有左恒等元，又有右恒等元，那么A有恒等元。

事实上，设e和e'分别是A的左恒等元和右恒等元，则

$$e = ee' = e'$$

故e是A的恒等元。

同样还可推得：如果广群A有恒等元，那么A的恒等元唯一。

例 1　$\{Z;\ +\}$，$\{Q;\ +\}$，$\{R;\ +\}$，$\{C;\ +\}$中的 0 是恒等元。

$\{N;\ \cdot\}$，$\{Z;\ \cdot\}$，$\{Q;\ \cdot\}$，$\{R;\ \cdot\}$，$\{C;\ \cdot\}$中的 1 是恒等元。

$\{S_n;\ \cdot\}$中的恒等变换$I=(1)$，$\{Z_m;\ +\}$中的$\overline{0}$，$\{Z_m;\ \cdot\}$中的$\overline{1}$，$\{M_n(F);\ +\}$中的零阵，$\{M_n(F);\ \cdot\}$中的单位阵都是恒等元。

例 2　$\{N;\ +\}$既无左恒等元也无右恒等元。

事实上，若e是N的左恒等元，则$\forall a\in N$有

$$e + a = a$$

于是推得$e=0$。但$0\overline{\in}N$，故N无左恒等元。同理，N也无右恒等元。

例 3　设 $A=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle|\ a,b\in R\right\}$

$$B=\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle|\ a,b\in R\right\}$$

A，B关于矩阵乘法都构成半群，其中A有左恒等元：$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$，但无右恒等元。$B$有右恒等元：$\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}$，但无左恒等元。本例的详细说明在学习指导中给出。

定义 5 有恒等元的半群叫做亚群。

例 1 中的代数体系都是亚群。

定义 6 设 A 是亚群，S 是 A 的子集。如果 S 关于 A 的乘法也构成亚群，而且 A 的恒等元是 S 的恒等元，则 S 叫做 A 的子亚群。

广群或半群 A 的子集 S 关于 A 的乘法构成亚群时，S 也叫做 A 的子亚群。

例 4 设 A 是任一非空集合，$T(A)$ 是 A 的所有变换的集合。S_n 是所有 n 元置换的集合。关于变换乘法，$T(A)$ 和 S_n 都构成亚群。当 A 是 n 元有限集合时，S_n 是 $T(A)$ 的子亚群。

Z_6 和其子集 $S=\{\overline{0}, \overline{3}\}$ 关于剩余类乘法都构成亚群，它们都有恒等元。但是 Z_6 的恒等元 $\overline{1}$ 不是 S 的恒等元，S 的恒等元是 $\overline{3}$，所以 S 不是亚群 Z_6 的子亚群。

与半群的情形相同，同态、同构在亚群理论中有着重要作用。

定理 4 设 $\{A; \circ\} \overset{\varphi}{\sim} \{B; \circ'\}$，如果 A 是亚群，则 B 必是亚群。

证明 设 A 是亚群，当然 A 是半群，由本节定理 3 知，B 是半群。下面证明 B 有恒等元。设 e 是 A 的恒等元，令 $\varphi(e)=e'$，则 e' 就是 B 的恒等元。

事实上，$\forall a' \in B$，由于 φ 是满射，有 $a \in A$ 使 $\varphi(a)=a'$，于是

$$e' \circ' a' = \varphi(e) \circ' \varphi(a) = \varphi(e \circ a) = \varphi(a) = a'$$

$$a' \circ' e' = \varphi(a) \circ' \varphi(e) = \varphi(a \circ e) = \varphi(a) = a'$$

因此 B 是亚群。证完。

此定理表明，亚群的同态象是亚群，而且从定理的证明过程中看到，恒等元的象是恒等元。与定理 3 相似，定理 4 的逆命题不真（见定理 3 下面所举的反例），但有如下结果。

推论 设 $\{A; \circ\} \cong \{B; \circ\}$，则 A 是亚群 $\Longleftrightarrow B$ 是亚群。

习　　题

1　设 $A=\{a,b,c\}$，试对A定义运算“$\circ_1$”和“$\circ_2$”，使得“$\circ_1$”满足交换律，A 关于“$\circ_2$”具有恒等元。这两个运算的运算表各有哪些特征？

2　试对$A=\{a,b,c,d\}$定义运算“$\circ$”使得$\{A;\ \circ\}$是交换亚群。

3　对$\mathbf{R}$定义运算

$$\circ:\ a\circ b=a+b-ab,\ \forall a,b\in\mathbf{R}$$

其中等号右端里的运算是数的加法、减法和乘法。证明：$\{\mathbf{R};\ \circ\}$ 是亚群。

4　证明$\{\mathbf{R};\ +\}$与$\{\mathbf{Z};\ +\}$不同构。

第二章　群

在第一章中我们给出了代数体系的概念，各式各样的代数体系构成了近世代数的主要研究对象，其中最简单的代数体系就是群。它是具有一个代数运算且满足某些条件的完整的代数体系，形成近世代数的一个独立的重要分支。通过这一章的学习将使我们初步了解近世代数研究问题的基本方法和格式，也为学习以后各章打下必要的基础。

§1　群的定义

在这一节中我们将给出群的定义、基本性质、例子以及与定义等价的几个命题。

定义　代数体系$\{G;\ \cdot\}$如果满足条件

（1）结合律成立

$$a(bc)=(ab)c,\quad \forall a,b,c\in G$$

（2）G中存在恒等元e；

（3）对G中每一元素a，在G中存在元素a'，使

$$a'a=aa'=e$$

称元素a'为a的逆元。则称代数体系$\{G;\ \cdot\}$是一个群，或简称G为群。

显然，群是特殊的半群和亚群。所以凡半群、亚群所具有的性质，群均具有。此外，群还具有一些一般半群、亚群所不具备的性质。归纳起来群有如下几条基本性质。

1　群中存在唯一的恒等元e。

2　群中每一元有且只有一个逆元。

事实上，若 a 有两个逆元a'，a''，即 $a'a=aa'=e$，$a''a=aa''=e$。那么

$$a'=ea'=(a''a)a'=a''(aa')=a''e=a''$$

以后把 a 的唯一的逆元用 a^{-1}表示．显然，a 是 a^{-1}的逆元，即$(a^{-1})^{-1}=a$。

易证$(ab)^{-1}=b^{-1}a^{-1}\quad\forall a,b\in G$，一般地有

$(a_1a_2\cdots a_n)^{-1}=a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}$（请读者自证之）

3　群中乘法“·”满足广义结合律（证明见第一章§6定理1）。

4　指数律成立。

我们可以在群中定义幂的概念．当$a_1=a_2=\cdots=a_n=a$时，把 n 个 a 自乘所得的结果记作a^n，即

$$\overbrace{aa\cdots a}^{n个}=a^n$$

而把 n 个a^{-1}之积记作a^{-n}，即

$$\overbrace{a^{-1}a^{-1}\cdots a^{-1}}^{n个}=a^{-n}\text{（其中 }n\text{ 为正整数）}$$

并且规定：$a^0=e$

于是容易证明指数律

$$a^m\cdot a^n=a^{m+n},\quad (a^n)^m=a^{nm}$$

对任意整数 m，n 皆成立。

如果$ab=ba$，则有

$$(ab)^m=a^mb^m$$

5　消去律成立。

左消去律：若$ax=ay$，则$x=y$；

右消去律：若$xa=ya$，则$x=y$。

其中 a 是群G的任一元素。

这只要用 a 的逆元 a^{-1}从左（右）边乘上式，便可将 a 消掉。由

$$a^{-1}(ax)=a^{-1}(ay)$$

因为群的乘法满足结合律，所以有

$$(a^{-1}a)x=(a^{-1}a)y, \text{ 即 } ex=ey, \quad x=y$$

当群 G 的运算满足交换律时，称 G 为**交换群**，或**阿贝尔(Abel)群**。我们也常把交换群的运算叫做加法，并记为"+"，在这种说法下称该群为**加群**。而把恒等元叫做**零元**，用 0 表示。元素 a 的逆元 a^{-1}，叫做 a 的**负元**，用 $-a$ 表示。

对于加群来说，一个元素的方幂 a^n 就是这个元素的倍数 na，因此

$$na=\overbrace{a+a+\cdots+a}^{n\text{个}}$$

$$(-n)a=\overbrace{(-a)+(-a)+\cdots+(-a)}^{n\text{个}}=n(-a)$$

$$0a=0$$

指数律相应地改写为倍数律

$$ma+na=(m+n)a$$

$$m(na)=mna$$

$$m(a+b)=ma+mb$$

当群 G 只含有限个元素时，则称 G 为**有限群**，否则称 G 为**无限群**。有限群 G 的元素个数 n 叫做 G 的阶，无限群的阶规定为 ∞。

下面看几个例子。

例 1 $\{1, -1\}$ 对数的乘法作成有限交换群。

例 2 $\{Z; +\}$，$\{Q; +\}$，$\{R; +\}$，$\{C; +\}$，$\{\dot{Q}; \cdot\}$，$\{\dot{R}; \cdot\}$，$\{\dot{C}; \cdot\}$，$\{M_n(F); +\}$，$\{F[x]; +\}$，$\{V_n(F); +\}$ ($V_n(F)$ 表示数域 F 上 n 维向量空间）都是无限交换群。

例 3 $M_n(R)$ 为实数域 R 上 n 阶方阵的集合，"·"为 n 阶方阵的乘法，显然 $\{M_n(R); \cdot\}$ 满足群的定义中的前两条，

但不满足第3条．对于恒等元E（n阶单位阵)来说，不是每一个n阶方阵均有逆元（即逆阵），所以代数体系$\{M_n(\mathbf{R});\cdot\}$不是群，而只是亚群．但其中可逆方阵的集合

$$GL_n(\mathbf{R})=\{A\in M_n(\mathbf{R})\mid |A|\neq 0\}$$

对方阵乘法作成无限非交换群($n>1$)．

这是因为，$\forall A, B\in GL_n(\mathbf{R})$，$|A|\neq 0$，$|B|\neq 0$，而$|AB|=|A|\cdot|B|\neq 0$，故$AB\in GL_n(\mathbf{R})$．因此，$GL_n(\mathbf{R})$对方阵乘法封闭，$\{GL_n(\mathbf{R});\cdot\}$是一个代数体系．

（1）结合律显然成立；

（2）单位阵 $E\in GL_n(\mathbf{R})$是恒等元；

（3）对任意$A\in GL_n(\mathbf{R})$，A有逆阵$A^{-1}\in GL_n(\mathbf{R})$使

$$A^{-1}A=AA^{-1}=E$$

故$\{GL_n(\mathbf{R});\cdot\}$是一个群．且当$n>1$时为无限非交换群，称这个群为**一般线性群**．

例4　已知Z_6是以6为模的剩余类集合，对于剩余类的加法是一个代数体系．且满足结合律和交换律，$\overline{0}$是零元，每一元素均有负元，$\overline{0}$的负元是$\overline{0}$，$\overline{1}$和$\overline{5}$互为负元，$\overline{2}$和$\overline{4}$互为负元，$\overline{3}$的负元是自身，故$\{Z_6;+\}$是有限交换群．

一般地，$\{Z_n;+\}$也是有限交换群，其元素$\overline{i}$的负元为$\overline{n-i}$．称$\{Z_n;+\}$为以n为模的剩余类加群．

群还有以下几个等价定义，在验证一个非空集合是不是群时，可根据具体情况使用其中之一．

定理1　代数体系$\{G;\cdot\}$是群的充要条件是$\{G;\cdot\}$满足

（Ⅰ）结合律成立；

（Ⅱ）G中有一个左恒等元e，使

$$ea=a,\quad\forall a\in G$$

（Ⅲ）对G的每一个元素a，在G中a有左逆元a'，使

$$a'a=e$$

证明　必要性是明显的．只证充分性．

若$\{G;\ \cdot\}$满足（Ⅰ）、（Ⅱ）、（Ⅲ），往证$\{G;\ \cdot\}$是群．根据定义只须证明，$\{G;\ \cdot\}$满足群定义条件中的（2）和（3）即可。

先证（3）成立，即证明a的一个左逆元a'也一定是a的右逆元，亦即由$a'a=e$去证$aa'=e$。

因为由（Ⅲ），a'也有左逆元a''，使

$$a''a' = e$$

所以

$$aa' = e(aa') = (a''a')(aa') = a''[(a'a)a']$$
$$= a''(ea') = a''a' = e$$

再证（2）成立，即证明一个左恒等元也一定是一个右恒等元，亦即$\forall a\in G$，$ae=a$。

因为

$$ae = a(a'a) = (aa')a = ea = a$$

于是G有恒等元e。故$\{G;\ \cdot\}$是一个群．证完。

定理 2　代数体系$\{G;\ \cdot\}$是群的充要条件是$\{G;\ \cdot\}$满足

（Ⅰ′）结合律成立；

（Ⅱ′）对于G的任意两个元素a，b，方程

$$ax=b \quad 和 \quad ya=b$$

都在G中有解。

证明　必要性．若G是群，对于$a\in G$由定义中的（3），存在$a^{-1}\in G$，从而有$a^{-1}b\in G$．因为

$$a(a^{-1}b) = (aa^{-1})b = eb = b$$

故$a^{-1}b$是方程：$ax=b$的解．同样，ba^{-1}是方程

$$ya=b$$

的解。

充分性．若$\{G;\ \cdot\}$满足（Ⅰ′），（Ⅱ′），我们去证明$\{G;\ \cdot\}$是群．这只要由（Ⅰ′）、（Ⅱ′）证明$\{G;\ \cdot\}$满足定理 1 中的（Ⅱ）、（Ⅲ）就行了。

先证（Ⅱ）成立，即证G有左恒等元e。由（Ⅲ′），对于G中一个固定元素b，方程

$$yb=b$$

在G中有解。任取$yb=b$的一个解为e，则

$$eb=b \qquad (1)$$

下面证明此元素e是G的左恒等元，为此只需证对G中任意元素a，均有$ea=a$即可。

由（Ⅱ′）方程

$$bx=a$$

在G中有解c，使

$$bc=a \qquad (2)$$

由式（1）、（2）和（Ⅰ′），有

$$ea=e(bc)=(eb)c=bc=a$$

于是证明了G存在左恒等元e，这就推得了（Ⅱ）。

再证（Ⅲ）成立，即证对于G中每一元素a，在G中有左逆元a'，使$a'a=e$，这里的e是上面取定的左恒等元e。

任取$a\in G$，由（Ⅲ′）方程

$$ya=e$$

在G中有解a'，即每一元素a都有左逆元，这就推得了（Ⅲ）。证完。

由群中消去律成立，显然方程

$$ax=b \quad 和 \quad ya=b$$

在G中只有唯一解。

以上两个和群的定义等价的命题，在判断一个非空集合G，对于所给的代数运算是否是群时，有时是很方便的。

例 5 $\{S_3;\cdot\}$是三元置换对于置换乘法构成的代数体系。已知$\{S_3;\ \cdot\}$做成有恒等元$e=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$的半群。下面要验证$\{S_3;\ \cdot\}$是否为群，只要验证$S_3$的每一元均有左逆元即可。

任取$\begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix} \in S_3$，有$\begin{pmatrix} i_1 & i_2 & i_3 \\ 1 & 2 & 3 \end{pmatrix} \in S_3$，使

$$\begin{pmatrix} i_1 & i_2 & i_3 \\ 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

故由定理 1 知$\{S_3; \cdot\}$是群．称 S_3 为三次置换群（或三次对称群）.它共有 6 个元素，可用轮换表示如下：

$$(1),\quad (12),\quad (13),\quad (23),\quad (123),\quad (132)$$

由于

$$(12)(13) = (132),\quad (13)(12) = (123)$$

所以S_3是非交换群．这是我们看到的第一个有限非交换群的例子．以后可以证明（见本章 § 6 习题 8）S_3是阶数最小的有限非交换群.

例 6 有理数集Q，规定“$\circ$”如下

$$a \circ b = a + b + ab$$

试问$\{Q; \circ\}$ 是否构成群？

解 显然对任意$a, b \in Q$，$a \circ b$ 是 Q 中唯一确定的数，所以$\circ$是Q的代数运算．下面验证代数体系$\{Q; \circ\}$是否满足群的定义条件.

$$\begin{aligned}(a \circ b) \circ c &= (a + b + ab) \circ c = (a + b + ab) + c + \\ &\quad (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc \\ a \circ (b \circ c) &= a \circ (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + ab + ac + bc + abc\end{aligned}$$

故

$$a \circ (b \circ c) = (a \circ b) \circ c,\quad \forall a, b, c \in G$$

不难看出数零为$\{Q; \circ\}$ 的恒等元.

$\forall a \in Q$，a 是否有逆元呢？需看方程

$$a \circ x = 0$$

在Q中是否有解．由于$a\circ x=a+x+ax=0$，即$(1+a)x=-a$，所以当$a\neq-1$时，$a\circ x=0$有解为$-\frac{a}{1+a}$．即$a\neq-1$时，a有逆元为$-\frac{a}{1+a}$；当$a=-1$时，$\forall\ x\in Q$，因为$(-1)\circ x=-1+x-x=-1\neq0$，可见$-1$无逆元．故$\{Q;\ \circ\}$不是群．易证$Q\backslash\{-1\}$关于"$\circ$"运算却做成一个群(请读者作为练习)．

例 7　$G=\{a,\ b,\ c\}$，其乘法由下表规定

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

证明：$\{G;\ \cdot\}$是一个交换群．

证明　由上表可以看出"$\cdot$"确为G的一个代数运算；a是G的恒等元；每个元素都有逆元，a的逆元是a，b与c互为逆元．

下面验证"$\cdot$"满足结合律：

$$(xy)z=x(yz) \qquad (*)$$

因为（*）式的x，y，z都要取遍a，b，c，所以（*）式共有$3^3=27$个，这样就需对（*）式验证27次．但是由于a是恒等元，故$ax=xa=x$，$\forall x\in G$均成立．这样，三个元中只要出现a，则（*）式一定成立．因此，只需验证x，y，z分别取b，c的情形．这时，（*）式尚有$2^3=8$个，即以下8个

$$(bb)b=b(bb),\quad (bb)c=b(bc),\quad (bc)c=b(cc)$$

$$(bc)b=b(cb),\quad (cc)c=c(cc),\quad (cc)b=c(cb)$$

$$(cb)b=c(bb),\quad (cb)c=c(bc)$$

这里，只验证第二个，其余留做练习。

$$(bb)c = cc = b, \quad b(bc) = ba = b$$

故

$$(bb)c = b(bc)$$

因此，$\{G; \cdot\}$ 是一个群。由乘法表显然可知“·”满足交换律，所以$\{G; \cdot\}$是交换群。

由于有限群在群论里所占的地位极其重要，因此，最后再讨论一下有限群的性质。

我们知道一个群一定是半群，且消去律成立，但是，一个消去律成立的半群却未必是群。例如，$\{\dot{Z}; \cdot\}$ 为非零整数关于数的乘法作成的代数体系。显然它是一个半群，且消去律成立，但$\dot{Z}$中除± 1外，其它元均没有逆元，所以$\{\dot{Z}; \cdot\}$ 不是群。但对于有限半群来说，情形就不同了。

定理 3　一个有限半群$\{G; \cdot\}$ 是群的充要条件是消去律成立。

证明　必要性是显然的。下面证明充分性。只需证明$\{G; \cdot\}$满足定理 2 中的（Ⅰ′）即可。

先证明方程

$$ax = b, \quad \forall a, \ b \in G$$

在G中有解。

设$G = \{a_1, a_2, \cdots, a_n\}$ 共有 n 个元，用其中任意元 a 左乘G的所有元a_i，由于G对运算封闭，而得到G的子集

$$G' = \{aa_1, aa_2, \cdots, aa_n\} \subseteq G$$

而且当 $i \neq j$ 时，$aa_i \neq aa_j$，否则由消去律有 $a_i = a_j$，与G有 n 个元的假定不符。因此G'有 n 个不同的元，于是

$$G' = G$$

这样一来，必有$a_k \in G$，使

$$b = aa_k$$

这就是说，a_k是方程$ax = b$的解。

同理可证方程

$$ya = b$$

在G中有解。证完。

由这个定理可得有限群的等价定义：**一个非空的有限集合G是群，如果**

（i）$\{G;\ \cdot\}$是一个半群；

（ii）在G中消去律成立。

习　　题

1　设$G=\mathbf{Z}$，对G规定“$\circ$”如下

$$a\circ b=a+b-3$$

证明：$\{G;\ \circ\}$是一个群。

2　设$G=\{(a,\ b)\mid a,\ b\in\mathbf{R},\ a\neq 0\}$，规定

$$(a,\ b)\cdot(c,\ d)=(ac,\ ad+b)$$

证明：$\{G;\ \cdot\}$是一个群。

3　设$\{G;\ \cdot\}$是一个代数体系，则$\{G\times G;\ \circ\}$也是一个代数体系，这里$G\times G$中的运算“$\circ$”规定为

$$(a_1,\ a_2)\circ(b_1,\ b_2)=(a_1\cdot b_1,\ a_2\cdot b_2)$$

证明：当$\{G;\ \cdot\}$是群时，$\{G\times G;\ \circ\}$也是群。

4　证明：代数体系$\{G;\ \cdot\}$是群的充要条件是$\{G;\ \cdot\}$满足条件

（1）结合律成立；

（2）G中有一个右恒等元，使

$$ae=a\qquad \forall a\in G$$

（3）对G的每一个元素a，在G中a有右逆元a'，使

$$aa'=e$$

5　设G是一个群，s是G的一个固定元素，在G中规定运算

$$a\circ b=asb$$

证明：$\{G;\ \circ\}$是一个群。

6　设G是一个半群，且左、右消去律成立，则G是交换半群的充要条件是，$\forall a,\ b\in G$，$(ab)^2=a^2b^2$。

7　假设群G中每个元素都满足方程

$$x^2=e$$

证明：G是交换群。

8　证明：任意偶数阶有限群G必含有元素$a\neq e$，使$a^2=e$，且此种元素个数必为奇数。

9　设G是一个群，a，b，$c\in G$，证明

$$xaxba=xbc$$

在G中有且仅有一个解。

10　试证在任意阶大于2的非交换群中，存在满足$ab=ba$的两个异于恒等元的元素a，b。

§2　子　　群

为了搞清楚一个代数体系的结构常常需要研究它的子体系，这是近世代数研究问题的一种重要方法。研究一个群也常常利用它的具有某种性质的子集——子群去推测整个群的构造。所以对群的子群的研究在群论中是一个非常重要的课题。

在第一章§6中已经给出了一个半群（亚群）的子半群（子亚群）等概念，关于群自然地可以给出子群的概念。

定义　群$\{G;\ \cdot\}$的非空子集H，如果对于G的运算也作成群，则称H为G的**子群**。

例1　任何群G都有两个明显的子群。一个是由恒等元组成的$\{e\}$，一个是G本身。这两个子群称为G的平凡子群，其余的非平凡子群称为G的**真子群**。

例2　整数加群$\{\mathbf{Z};\ +\}$中的全体偶数作成的子集$\mathbf{Z}_0$，关于整数加法显然作成$\{\mathbf{Z};\ +\}$的子群。

例3　行列式等于1的全体实n阶方阵的集合

$$SL_n(R)=\{A\in M_n(R)\mid |A|=1\}$$

对矩阵乘法组成一个群，是全体可逆实方阵所作成的一般线性群$GL_n(R)$（见本章§1例3）的子群，称做特殊线性群。

例4　$\{R^+;\ \cdot\}$（R^+表示正实数集）和$\{1,\ -1\}$都是$\{\dot{R};\ \cdot\}$的子群，但$\{R^+;\ \cdot\}$不是$\{R;\ +\}$的子群，因运算不同。

需要注意的是，G的子群H不只是一个包含在G中的群，两者运算必须一样.

群G的子集H满足什么条件才能成为G的子群呢？

如果H是G的子群，首先G的运算必须是H的运算. 即$\forall a, b \in H$，其积 $ab \in H$，H对G的运算封闭. 其次来考察群的三个条件. 因为H包含在G中，所以结合律对H当然成立，这一条可以不必验证. 剩下只需检验另外两条，而这两条又可精减为一条，即下面的判定条件.

判别条件 1　群G的非空子集H作成G的子群的充分必要条件是

（1）$\forall a, b \in H \Longrightarrow ab \in H$；

（2）$\forall a \in H \Longrightarrow a^{-1} \in H$

证明　充分性. 只须证明 $e \in H$即可. $\forall a \in H$；由（2）推得$a^{-1} \in H$，再由（1）推得 $aa^{-1} = e \in H$，所以H是群，从而是G子群.

必要性. 因为H是G的子群，（1）显然成立. 只需证明（2）成立. 因H是群，设 e'是H的恒等元. $\forall a \in H$，有$e'a = a$. 但 e'，a都属于G，故e'是方程$ya = a$在G中的解. 而方程 $ya = a$ 在G中有且仅有一解为G的恒等元e，故$e = e' \in H$. 同理，方程 $ya = e$ 在H中有解为 a'，而 a' 也是这个方程在G中的解，显然这个方程在G中有且仅有一解，就是 a^{-1}. 故$a^{-1} = a' \in H$. 证完.

由上述必要性的证明中立即得到：

群G的子群H的恒等元就是G的恒等元，H中任意元素a在H中的逆元就是a在G中的逆元.

判别条件 2　群G的非空子集H是G的子群的充分必要条件是

$$\forall a, b \in H \Longrightarrow ab^{-1} \in H$$

证明　充分性. 因为H非空，所以有 $a \in H \to aa^{-1} = e \in H$. 进一步，$ea^{-1} = a^{-1} \in H$. 若$a, b \in H$，因$b^{-1} \in H$，故$a(b^{-1})^{-1} = ab$

116

$\in H$，所以，根据判别条件1，H是G的子群。

其次证明必要性。

设H是群G的子群，$\forall b\in H$，由判别条件1之（2）有$b^{-1}\in H$，所以，$\forall a, b\in H$，因$b^{-1}\in H$由判别条件1之（1）有$ab^{-1}\in H$。证完。

如果H是群G的有限子集，那么H作成G的子群的条件还可更简单一些。因为，在群中消去律成立。由有限群的定义，只要求G的运算对H封闭即可。于是又有

判别条件3　群G的非空有限子集H作成G的子群的充分必要条件是

$$\forall a, b\in H \Longrightarrow ab\in H$$

显然G的子群H的子群K也是G的子群，即子群有传递性。

例5　令V是平面上所有向量关于向量的加法所作成的加群，H是过原点的某定直线上的向量全体，则H是V的子群。显然，$\forall x, y\in H$，有$x+y\in H$，$-x\in H$，由判别条件1知H是V的子群。

例6　在整数加群$\{Z; +\}$中给定任意一个整数n，由n的一切倍数组成的集合

$$H=\{kn \mid k\in Z, n\text{为固定整数}\}$$

可证H为$\{Z; +\}$的子群。

事实上，$\forall k_1n, k_2n\in H$，有 $k_1n-k_2n=(k_1-k_2)n\in H$，由判别条件2知$H$是$\{Z; +\}$的子群。

例7　$G=S_3$，$H=\{(1), (12)\}$，则H是S_3的子群。

由H的乘法表

·	(1)	(12)
(1)	(1)	(12)
(12)	(12)	(1)

可知，H对于G的运算是封闭的，由判别条件3可知H为G的子群。

例8 若H_1，H_2为G的子群，则 $H_1 \cap H_2$也是G的子群。

显然$e \in H_1 \cap H_2$，故 $H_1 \cap H_2$ 非空。$\forall a$，$b \in H_1 \cap H_2$，则 a、$b \in H_1$，a、$b \in H_2$，由H_1、H_2 是子群，故 $ab^{-1} \in H_1$，$ab^{-1} \in H_2$，从而 $ab^{-1} \in H_1 \cap H_2$。故 $H_1 \cap H_2$ 是G的子群。此结果可推广为：群G的任意多个子群的交仍是G的子群。

最后介绍一种构造子群的一般方法。在群G中任取一个非空子集S。如果S不是群，由子群的判别条件1，可在S的基础上将它扩大，把做为一个群应该包含的元素都添进去（不止一次地添加），使其任二元素之积以及任一元素的逆元仍在其中，直至得到一个包含S的子群时为止。

设 $S=\{a_1,a_2,a_3,\cdots\}$，利用S的元素和它们的逆元做一切可能的乘积，比如

$$a_1a_2,\ a_1^{-1}a_3^{-1}a_2a_4^{-2},a_2^2a_3,\ a_3,\ a_4^{-1},\cdots$$

把所有这些元素都添加于S。于是得到G的子集

$$H=\{a_{i_1}^{k_1}a_{i_2}^{k_2}\cdots a_{i_n}^{k_n}\ |a_{i_j}\in S,k_j=\pm 1,n=1,2,\cdots\}$$

即H是一切形如

$$a_{i_1}^{k_1}a_{i_2}^{k_2}\cdots a_{i_n}^{k_n} \qquad (*)$$

的元素构成的。

因为任意两个（*）形的元素的乘积仍是（*）形的元素，（*）形元素的逆元也是（*）形的元素。于是，由判别条件1知，H是G的子群。

显然 $H \supseteq S$。在G中，除G和H外，可能还有其它子群也包含S。但是任一包含S的子群K都必包含H。事实上，因为K是一个子群，所以必须满足判别条件1中的条件（1）、（2）。由于$K \supseteq S$，K必包含所有（*）形的元，所以$K \supseteq H$。即H是G中所有包含S的子群的交集，显然H是G中包含S的最小子群。

这个由S决定的子群H叫做由S生成的子群。记作 $H=$

(S)。S 叫做 H 的生成元系，S中的元叫做 H 的生成元。当 S 本身是子群时，显然有 $(S)=S$。当 $S=\{a_1,a_2,\cdots,a_n\}$ 为G的有限子集，且$a_ia_j=a_ja_i$时，则

$$H=(S)=\{a_1^{m_1}a_2^{m_2}\cdots a_n^{m_n}\mid a_i\in S, m_i\in Z\}$$

特别地，当$S=\{a\}$，由一个元 a 生成的子群记为（a），它是由 a 的所有幂a^n形成的。这种群将在本章 § 4 作重点讨论。

例 9　在$GL_2(R)$（见 § 1 例 3）中，取两个阵

$$a=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\qquad b=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$$

试确定由$S=\{a,b\}$生成的子群H。

解　因为，由a，b生成的子群运算必须封闭，所以其中必含有下列元素

$$ab=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=c$$

$$a^{-1}=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=a,\ aa^{-1}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=e$$

$b^{-1}=b$，$c^{-1}=c$，$ac=b$，$bc=a$

$ba=c$，　$ca=b$，　$cb=a$

通过做各种可能的乘积，共得四个元素的集合

$H=\{e,a,b,c\}$

由其乘法表

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

可以看出

（1） H关于矩阵乘法封闭；

（2） 每一元素均有逆元皆为自身。

故H为由 S 生成的$GL_2(R)$的子群，即 $H=(S)$，其阶为 4。

习　　题

1　设S是群G的一个子集，令

$$C(S)=\{x\in G\mid\forall s\in S,\ xs=sx\}$$

证明：$C(S)$是G的子群，$C(S)$叫做S的中心化子。特别地，当 $S=G$时，$C(G)$叫做G的中心。

2　设S是群G的子集，令

$N(S)=\{x\mid x\in G,\ xSx^{-1}=S\}$，其中，$xSx^{-1}=\{xsx^{-1}\mid s\in S\}$

则$N(S)$是G的子群。$N(S)$叫做S的正规化子。S的中心化子$C(S)$与正规化子$N(S)$有何不同？

3　设G为交换群，m为一固定整数，令

$$G^{(m)}=\{a^m\mid a\in G\},\quad G_{(m)}=\{a\in G\mid a^m=e\}$$

证明：$G^{(m)}$和$G_{(m)}$都是G的子群。

4　$H=\{x\mid x\in\dot{C},$ 存在某个自然数n，使$x^n=1\}$。证明：H是 $G=\{\dot{C},\ \cdot\}$的子群。

5　试证下面四个矩阵对于矩阵乘法运算作成群：

$$e=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad a=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\quad b=\begin{pmatrix}1&0\\0&-1\end{pmatrix},$$

$$c=\begin{pmatrix}-1&0\\0&1\end{pmatrix}$$

6　证明：S_3的子集

$$B_4=\{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

是S_3的子群，叫做克莱茵（Klein）四元群。

7　设H为G的子群，任取$a\in G$，则 aHa^{-1} 也是G的子群，且H与aHa^{-1}有相同的阶，称aHa^{-1}为H的共轭子群。

8　设H_i（$i=1,2,\cdots$）是G的一组子群，并且

$$H_1\subseteq H_2\subseteq\cdots\subseteq H_n\subseteq\cdots$$

(称$\{H_i\}$为子群的升链)则

$$H=\bigcup_{i\in I}H_i$$

是G的子群。

9　取S_3的子集$S=\{(12),(123)\}$。S生成的子群包含哪些元素?一个群的两个不同的子集会不会生成相同的子群?

10　在$GL_2(\boldsymbol{R})$(见§1例3)中,取两个二阶阵

$$a=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\quad b=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

试确定由$S=\{a,b\}$生成的子群H,其阶如何?

11　证明:群G的一个子集S是G的一组生成元,当且仅当G中不存在包含集合S所有元素的真子群。

12　证明:群G不能是它的两个真子群的并。

§3　群的同态、同构

在第一章§5中已经讨论了代数体系的同态、同构。本节将着重讨论群的同态、同构。这是研究群的构造的重要手段。

两个群$\{G;\circ\}$与$\{G';\circ'\}$做为代数体系,如果存在G到G'的映射φ,使得,$\forall a,b\in G$有

$$\varphi(a\circ b)=\varphi(a)\circ'\varphi(b)$$

则称φ为$\{G;\circ\}$到$\{G';\circ'\}$的**同态映射**,简称同态。

$\varphi(G)=im\varphi$,叫做G在φ之下的同态象。显然$\varphi(G)\subseteq G'$。

当φ为$\{G;\circ\}$到$\{G';\circ'\}$的满同态映射时,即$\varphi(G)=G'$,则称$\{G;\circ\}$与$\{G';\circ'\}$满同态,简记作$G\overset{\varphi}{\sim}G'$。

当$\{G;\circ\}$到$\{G';\circ'\}$的同态映射φ为双射时,则称φ是$\{G;\circ\}$到$\{G';\circ'\}$的一个**同构映射**。此时称$\{G;\circ\}$与$\{G';\circ'\}$同构。简记作$G\cong G'$。

显然同构映射是同态映射的特例。当$G=G'$时,同态映射φ叫做G的自同态,同构映射φ又叫G的自同构。

关于群的同态有如下的结论：

由第一章§6已经知道，如果$\{G;\circ\}$与$\{G';\circ'\}$满同态：$G\overset{\varphi}{\sim}G'$，则有

（1）G的运算"$\circ$"满足结合律$\Rightarrow G'$的运算"$\circ'$"满足结合律；

（2）G的运算"$\circ$"满足交换律$\Rightarrow G'$的运算"$\circ'$"满足交换律；

（3）G的元素e是一个恒等元$\Rightarrow e'=\varphi(e)$是$G'$的一个恒等元；

（4）设e为G的一个恒等元，由（3）G'中也有恒等元e'，而且就是$e'=\varphi(e)$，于是，当G中元素a有逆元b，则$a'=\varphi(a)$也有逆元，且恰为$b'=\varphi(b)$，即a的逆元b的象$\varphi(b)$是a的象a'的逆元。

事实上，设b为a的逆元，即$a\circ b=b\circ a=e$，令

$$a\longmapsto a'=\varphi(a),\quad b\longmapsto b'=\varphi(b)$$

由于φ为G到G'的同态映射，故

$$\varphi(a)\circ'\varphi(b)=\varphi(a\circ b)=\varphi(e)=e'$$

$$\varphi(b)\circ'\varphi(a)=\varphi(b\circ a)=\varphi(e)=e'$$

即 $\varphi(a)\circ'\varphi(b)=\varphi(b)\circ'\varphi(a)=e'$.故$a'=\varphi(a)$有逆元为：$b'=\varphi(b)$。

由上述（1）、（3）、（4）条可得：

定理 若$G\overset{\varphi}{\sim}G'$，$G$是群，则$G'$也是群。

即群的同态象仍是群。但定理的逆命题未必成立。例如，取$G=\{Z;\cdot\}$，$G'=\{1;\cdot\}$，令

$$\varphi;\ n\longmapsto 1$$

显然φ是G到G'的满同态映射：$G\overset{\varphi}{\sim}G'$。$G'$是群，但$G$不是群，因$G$中的元除$\pm1$外，其它元素没有逆元。

这说明，若$G\sim G'$，则由G的代数性质可知G'也有相应

的代数性质，反之未必成立.

但若φ是代数体系G到G'的同构映射，即$G\overset{\varphi}{\cong}G'$，则 G' 是群，G也是群。因为φ为双射，故为可逆映射，故φ有逆映射φ^{-1}。显然φ^{-1}是G'到G的同构映射，即$G'\overset{\varphi^{-1}}{\cong}G$。因此，由$G'$的代数性质可知$G$也有相应的代数性质。此时，$G$与 G' 代数运算的性质完全相同。我们把代数体系的代数性质的总合称为它的代数结构，因而从代数观点看，同构的群有完全相同的代数结构。除元素和运算符号的差异外，没有本质的不同，我们也常说它们是代数相等的。

推论 若 $G\overset{\varphi}{\cong}G'$，则$G$是群的充分必要条件是 G'是群。

例 1 $G=\{Z_3;+\}$（加群），$G'=\{1,\omega,\omega^2|\omega^3=1\}$（乘群），$G$和 G' 的运算表如下：

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

令φ：$\overline{0}\longmapsto 1$

$\overline{1}\longmapsto \omega$

$\overline{2}\longmapsto \omega^2$

显然φ是G到 G' 的双射。实际上这两个表按照元素的对应关系是一致的，所以彼此对应着的元素，其运算的结果也恰好对应着。用式子表示就是：$\varphi(a+b)=\varphi(a)\cdot\varphi(b)$，即$\varphi$保持运算关系不变。所以，$\varphi$是$G$到 G'的同构映射，即$G\cong G'$。

例 2 $G=\{R;+\}$是实数加群，$G'=\{R^+;\cdot\}$是正实数乘群。设

$$\varphi:\quad x\longmapsto 10^x$$

显然φ是G到G'的双射。 若令

$$y \longmapsto 10^y$$

则有

$$\varphi(x+y)=10^{x+y}=10^x \cdot 10^y=\varphi(x)\cdot\varphi(y)$$

故$G \cong G'$。

此二例中的两个集合尽管不同，运算也各异，而从代数观点看，它们没有本质的不同。

例 3 证明：$G=\{\dot{R};\ \cdot\}$与$G'=\{R;\ +\}$不同构。

证明 用反证法。假如G与G'同构，可设φ为G到G'的一个同构映射，于是由群同态的性质必有

$$\varphi;\ 1 \longmapsto 0,\quad -1 \longmapsto a,\quad a \neq 0$$

从而

$$\varphi(1)=\varphi((-1)\cdot(-1))=\varphi(-1)+\varphi(-1)=2a$$

但$\varphi(1)=0$，故$2a=0$，于是$a=0$，此矛盾说明$\{\dot{R};\ \cdot\}$与$\{R;\ +\}$不能同构。

有时当需要判断一个代数体系G'是否为群时，除了按群的定义逐条验证外(有时是比较麻烦的)，如果能找到一个已知群G，证明二者同构$G \cong G'$或满同态$G \sim G'$，则可由G为群，推知G'也为群。

例 4 $G'=\{a,b,c\}$运算表如下

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

此G'即为§1例7中之G。当时判断G'为群时，证明结合律是相当麻烦的。现在只要仔细观察G'的运算表与我们所熟知的$G=\{Z_3;\ +\}$的运算表（见例1），就会发现它们之间的联系。事实上，令

$$\varphi: \ \overline{0} \longmapsto a, \ \overline{1} \longmapsto b, \ \overline{2} \longmapsto c$$

显然φ是G到 G' 的双射。因为这两个运算表完全重合，容易验证φ为G到G'的同构映射，即$G \cong G'$。故由G为群推知 G' 也为群。

我们研究群（其它代数体系也同样）的首要目的就是要确定所有不同构的群的代数结构。实际上确定一个群（抽象群）的代数结构，只要让它与一个代数结构已经清楚了的具体群同构即可。如果能做到这一点，那么这个抽象群的代数结构就清楚了。在下一节中我们将给出一个研究群的代数结构的“范例”。

习　　题

1　证明：整数加群$\{\boldsymbol{Z};\ +\}$与偶数加群同构。

2　设$G = GL_n(\boldsymbol{R})$，　$G' = \{\dot{\boldsymbol{R}};\ \cdot\}$，证明：$G \sim G'$。

3　设$G = \{\boldsymbol{R};\ +\}$为加群，$G' = \{e^{i\theta} | \theta \in R\}$为具有乘法运算的代数体系。在映射

$$\varphi: \theta \longmapsto e^{i\theta}$$

之下，G与G'是否同构，又是否满同态，$\{G';\ \cdot\}$是否为群？

4　已知$G = \{1,\ i,\ -1,\ i\}$ 为群，$G' = \{\sigma_0,\ \sigma_{\frac{\pi}{2}},\ \sigma_{\pi},\ \sigma_{\frac{3\pi}{2}}\}$，这里$\sigma_i$是绕一固定直线旋转 i 弧度的空间旋转。试证G'也是一个群（不直接用定义证）。

5　设φ是G到G'的一个满同态，证明：G的中心 $C(G)$的元素在φ之下的象是G'的中心$C(G')$中的元素。

6　证明：G为可换群当且仅当映射

$$\varphi: \ a \longmapsto a^{-1}$$

是G的自同构。

7　若φ是群G到G'的同态映射，证明：

（1）若H是G的子群，则$\varphi(H)$是G'的子群；

（2）若H'是G'的子群，则$\varphi^{-1}(H') = \{x | x \in G,\ \varphi(x) \in H'\}$是$G$的子群。

§4 循环群

本节将讨论一种代数结构特别简单，而在群论中颇有代表性的群—循环群。

一般来说，对于一个代数体系如果能够解决这个体系的存在问题、数量问题、构造问题，那么这个代数体系就清楚了。对循环群来说，上述三个基本问题都作了肯定地回答。

在§2末曾讨论了由一个群的子集S生成的子群。当S只含一个元素，即$S=\{a\}$时，由S生成的子群(a)的构造特别简单。(a)的任意元素都是a的乘幂。现在我们要问：一个群G的元素会不会都是G的某一个固定元素a的乘幂？

例1　$\{Z;+\}$为整数加群。对于加群来说 a 的乘幂a^n即na（n为任意整数）。显然任意整数都是1的倍数（即1的"幂"），所以整数加群可以看做是由1生成的。显然，它也是由-1生成的，即$Z=(1)=(-1)$。

例2　$\{Z_n;+\}$是以n为模的剩余类加群。它的元素共有n个：$\overline{0}$，$\overline{1}$，$\overline{2}$，…，$\overline{i}$，…，$\overline{n-1}$。显然，$\overline{i}=i\cdot\overline{1}$，即任意元$\overline{i}$都是$\overline{1}$的倍数。$Z_n$是由$\overline{1}$生成的，即$Z_n=(\overline{1})$。

定义1　若一个群G是由其中某个元素a生成的，即$G=(a)$，则G叫做循环群，而称a为G的生成元。

显然按定义，例1、例2都是循环群。$\{Z;+\}$是无限循环群，$\{Z_n;+\}$为n阶有限循环群。由n的任意性，可知阶数为任意自然数n的循环群是存在的。

下面来讨论一下循环群的构造。

1　若a的所有的幂都互不相等，即$h\neq k$时，$a^h\neq a^k$。这时循环群(a)由下列元素组成：

$$\cdots,\ a^{-2},\ a^{-1},\ a^0,\ a^1,\ a^2\cdots$$

(a)为无限循环群。

2　若a的幂中有相等的，即存在$k\neq h\in Z$有$a^h=a^k$，不

妨设$h>k$．于是有

$$a^{h-k}=e, \qquad h-k>0$$

由此可知，对于a来说存在正整数m，使 $a^m=e$。

令n是使$a^n=e$的最小正整数，则(a)由如下n个不同元组成：

$$a^0, \ a, \ a^2, \ \cdots, \ a^{n-1} \qquad (1)$$

首先证明，（1）中n个元彼此互异。因为，如若

$$a^i=a^j, \qquad 0\leqslant j<i<n$$

那么

$$a^{i-j}=e, \qquad 0<i-j<n$$

这与n是使 $a^n=e$成立的最小正整数的假设矛盾。

其次证明，(a)中任一元 a^m（m为任一整数）必与（1）中某一元相等。把m写成

$$m=nq+r, \quad 0\leqslant r<n$$

于是有

$$a^m=a^{nq+r}=a^{nq}\cdot a^r=(a^n)^q\cdot a^r=ea^r=a^r$$

所以 a 的任意整数幂必与（1）中某一元相等。这就证明了(a)是含n个元

$$a^0, \ a, \ a^2, \ \cdots, \ a^{n-1}$$

的有限循环群。

从上面讨论可以看到，循环群(a)所含元素个数是无限还是有限，取决于a的幂是否有相等的。即对于不同的整数m和n来说，是否有$a^m=a^n$。而这一点又取决于是否存在最小正整数n，使$a^n=e$。因此，循环群$G=(a)$所含元素个数与是否存在满足上述条件的最小正整数n有着密切关系。在讨论循环群(a)的构造时，这个最小正整数n起着相当重要的作用。为此给出如下定义。

定义 2 对群G的元素a，若存在使

$$a^n=e$$

的最小正整数n，则称a的阶（周期）为n，若这样的n不存在，就说a是无限阶的（周期是无限的）。

例如，由四次单位根所构成的乘群$G=\{1,-1,i,-i\}$中，1的阶为1，-1的阶为2，i和$-i$的阶都是4；在$\{Z_6;\ +\}$中，$\overline{0}$的阶为1，$\overline{1}$和$\overline{5}$的阶为6，$\overline{2}$和$\overline{4}$的阶为3，$\overline{3}$的阶为2. 而在整数加群$\{Z;\ +\}$中任意非零的整数都是无限阶的.

下面我们给出循环群的构造定理.

定理1　设循环群 $G=(a)$，则 G 的构造完全由其生成元 a 的阶决定：

（1）若 a 的阶为无限，则G与整数加群同构；

（2）若 a 的阶为 n，则G与以 n 为模的剩余类加群同构.

证明（1）设 a 为无限阶的，$G=(a)=\{\cdots,a^{-2},a^{-1},a^0,a^1,a^2,\cdots\}$，这时

$$a^{m_1}=a^{m_2}\Longleftrightarrow m_1=m_2$$

事实上，若$m_1=m_2$，显然$a^{m_1}=a^{m_2}$. 反过来，若$a^{m_1}=a^{m_2}$，而$m_1\neq m_2$，可假定$m_1>m_2$，则有 $a^{m_1-m_2}=e$，这与 a 为无限阶的假设不符。令

$$\varphi:\ a^m\longmapsto m$$

由上讨论易知φ是(a)到$\{Z;\ +\}$的双射. 且

$$\varphi(a^m\cdot a^n)=\varphi(a^{m+n})=m+n=\varphi(a^m)+\varphi(a^n)$$

所以φ是(a)到$\{Z;\ +\}$的一个同构映射. 故 $(a)\cong\{Z;\ +\}$.

（2）设a的阶为n，$a^n=e$，则$G=(a)=\{a^0,a,a^2\cdots,a^{n-1}\}$，这时

$$a^{m_1}=a^{m_2}\Longleftrightarrow n\mid m_1-m_2$$

事实上，若$n\mid m_1-m_2$，则 $m_1-m_2=nq$，$m_1=nq+m_2$，于是

$$a^{m_1}=a^{nq+m_2}=(a^n)^q\cdot a^{m_2}=ea^{m_2}=a^{m_2}$$

如果$a^{m_1}=a^{m_2}$，令

$$m_1-m_2=nq+r,\qquad 0\leqslant r<n$$

那么

$$e=a^{m_1-m_2}=a^{nq+r}=(a^n)^q\cdot a^r=ea^r=a^r$$

由 a 的阶为 n，必有$r=0$，故$n|m_1-m_2$。规定

$$\varphi: a^k \longmapsto \overline{k}$$

显然φ是(a)到$\{Z_n; +\}$的映射。

下面证明φ是(a)到$\{Z_n; +\}$的双射。

任取 a^{m_1}，$a^{m_2}\in(a)$，若$a^{m_1}\neq a^{m_2}$，则 $\overline{m_1}\neq\overline{m_2}$，否则由 $\overline{m_1}=\overline{m_2}$，必有$n|m_1-m_2$，由上面讨论可知$a^{m_1}=a^{m_2}$与$a^{m_1}\neq a^{m_2}$矛盾。故$\varphi$是$(a)$到$\{Z_n; +\}$的单射。

显然φ是(a)到$\{Z_n; +\}$的满射。所以φ是(a)到$\{Z_n; +\}$的双射。而且

$$\varphi(a^k\cdot a^s)=\varphi(a^{k+s})=\overline{k+s}=\overline{k}+\overline{s}$$
$$=\varphi(a^k)+\varphi(a^s)$$

故φ为(a)到$\{Z_n; +\}$的一个同构映射。即

$$(a)\cong\{Z_n; +\}$$
证完。

这个定理说明，一个由 a 生成的循环群的构造完全由 a 的阶所决定。如果 a 的阶为无限，那么这个循环群和整数加群同构；如果 a 的阶为 n，那么这个循环群和 $\{Z_n; +\}$ 同构。因此有，**同阶循环群同构**。

研究群，还有一个很重要的问题，就是决定一个群的所有子群。这对任意群来说不是一件很容易的事，但对循环群来说，问题是不难解决的。

命题 1　循环群 $G=(a)$ 的子群H也是循环群。

证明　若$H=\{e\}$，则$H=(e)$，即H是循环群。若$H\neq\{e\}$，则H必含有$a^k\neq e$。$k\neq0$，这时必有$a^{-k}\in H$。所以，当$H\neq\{e\}$时，在H中一定含有 a 的某些正整数幂。在这些 a 的正整数幂中必有一个幂指数为最小者，令其为a^s，即若$0<h<s$，则$a^h\notin H$。下面证明a^s为H的生成元，即$H=(a^s)$。这只要证明H中的任意元 b 皆可表为 $b=(a^s)^q$即可。因$b\in H$，当然$b\in G$。令 $b=a^m$，由带余除法

$$m=sq+r,\quad 0\leqslant r<s$$

$$a^m = a^{sq+r} = a^{sq} \cdot a^r = (a^s)^q \cdot a^r$$

因 $a^m \in H$，$(a^s)^q \in H$，故 $a^r \in H$。又由 $0 \leqslant r < s$，及 s 的最小性，必有 $r = 0$。这样 $m = sq$，即 $a^m = (a^s)^q$。所以 $H = (a^s)$ 是由 a^s 生成的循环群，证完。

因为在群中

$$(a^t)^s = (a^s)^t$$

所以，当循环群 (a) 的子群 H 的生成元为 a^s 时，则 $H = (a^s)$ 恰由 (a) 中所有元的 s 次幂构成。

如果 a 的阶无限，显然 a^s 的阶也必无限 $(s > 0)$。这时，a^s 所生成的循环群由循环群 (a) 中下列元素构成：

$$\cdots,\ a^{-2s},\ a^{-s},\ a^0,\ a^s,\ a^{2s},\ \cdots$$

所以，无限循环群 (a) 的子群 $H \neq \{e\}$ 必是无限循环群。

对于无限循环群 $G = (a)$ 来说，当 s 和 t 是任意不同的非负整数时，则 (a^s) 和 (a^t) 是 $G = (a)$ 的不同子群。综上所述有

命题 2　无限循环群 $G = (a)$ 的子群除 $\{e\}$ 外都是无限循环群；在非负整数集与 $G = (a)$ 的所有子群的集合之间，有双射

$$s \longmapsto (a^s)$$

s 为非负整数。

对于有限循环群 $G = (a)$ 有

命题 3　设 $G = (a)$ 是 n 阶循环群 $(a^n = e)$，则

（1）G 的任意子群 H 的阶是 G 的阶的正约数；

（2）对于 n 的任一正约数 d，$G = (a)$ 有且只有一个阶为 d 的子群。

证明　令 a^s 为在命题 1 证明中所指出的 H 的生成元：$H = (a^s)$，即 s 是使 $a^s \in H$ 的最小正整数。我们先证明 $s \mid n$，由带余除法有

$$n = sq + r,\quad 0 \leqslant r < s$$

因为 $a^n = e$，而 $e = a^n = a^{sq+r} = a^{sq} \cdot a^r$，所以有

$$a^r = a^{-sq} = (a^s)^{-q} \in H = (a^s)$$

而 $0 \leqslant r < s$，所以由 s 的最小性必有 $r = 0$，即 $s \mid n$，令 $n = st$，

则有

$$H=(a^s)=\{(a^s)^0,\ a^s,\ a^{2s},\ \cdots,\ a^{(t-1)s}\}$$

即H的阶为 t，而 $t|n$，故（1）得证。

下面证明（2）成立。令$n=dr$，则(a^r)是 $G=(a)$的 d 阶子群。

事实上，因为$(a^r)^d=a^{rd}=a^n=e$，所以a^r的阶$\leqslant d$。而当 $0<k<d$ 时有 $0<rk<rd=n$，于是由题设 a 的阶为 n，有 $(a^r)^k\neq e$。即 d 是使$(a^r)^d=e$ 的最小正整数，故 a^r的阶为 d。从而(a^r)为 d 阶循环群。

最后证明$G=(a)$只有一个 d 阶子群。令H是$G=(a)$的d阶子群，往证$H=(a^r)$，$(n=rd)$。

由命题1知 H是循环群，而 $H\subseteq(a)$，令 a^t 是H的生成元，则$H=(a^t)$，因为H的阶为 d，所以a^t的阶是 d。令

$t=rq+s,\ 0\leqslant s<r$

则

$$e=(a^t)^d=a^{td}=a^{(rq+s)d}=a^{(rd)q}a^{sd}=a^{nq}a^{sd}=a^{sd}$$

由 $0\leqslant s<r$，有 $0\leqslant sd<rd=n$，而a的阶为n，所以由 $a^{sd}=e$ 必有$sd=0$。但$d>0$，故$s=0$。从而有：$t=rq$。于是得到：$a^t=a^{rq}=(a^r)^q\in(a^r)$。所以有$H=(a^t)\subseteq(a^r)$。

但H和 (a^r) 都是 $G=(a)$的 d 阶子群。故有 $H=(a^t)=(a^r)$，即$G=(a)$只有一个 d 阶子群。（2）得证。

把上面三个命题归纳起来，我们有

定理 2 （1）循环群 $G=(a)$的子群H都是循环群。若$H\neq\{e\}$，则H是由H中元a的最小正整数幂a^s生成的。（2）当$G=(a)$是无限群时，$H\neq\{e\}$也是无限群，而且，存在非负整数集到 $G=(a)$的所有子群构成的集的双射。（3）当 $G=(a)$ 为n阶有限群时，则 G的子群H的阶必为n的正约数，而且对于n的任一正约数d，$G=(a)$ 有且只有一个阶为d的子群。

例 3　令$U_n=\{\varepsilon_k\in C\,|\,\varepsilon_k^n=1\}$为$n$次单位根的集合。

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, k = 0,1,2,\cdots,n-1$$

易知$\{U_n; \cdot\}$是一个群，而且是由

$$\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

生成的循环群。

当取$n = 8$时，则因 8 的正约数共有 4 个：1,2,4,8.所以，由定理 2 可知U_8恰有 4 个子群.

$$H_1 = (\varepsilon_1^0),\ H_2 = (\varepsilon_1^4) = \{\varepsilon_1^0, \varepsilon_1^4 = \varepsilon_4\}$$

$$H_3 = (\varepsilon_1^2) = \{\varepsilon_1^0, \varepsilon_1^2, \varepsilon_1^4, \varepsilon_1^6\},\ H_4 = (\varepsilon_1) = U_8$$

最后再讨论一下循环群的同态象。

命题 4　若$G = (a)$，则G的同态象 G' 也是循环群，而且 G' 的生成元是G的生成元 a 的象.

证明　设$G = (a)$，$G \overset{\varphi}{\sim} G'$ 由 § 3 定理G是群知 G' 也是群。规定

$$\varphi: a \longmapsto a'$$

下面证明a'是G'的生成元. 任取G'中的元b',在G中b'有原象设为 b，使 $\varphi(b) = b'$. 因G为循环群，故 $b = a^m$，由$G \sim G'$知

$$b' = \varphi(b) = \varphi(a^m) = (\varphi(a))^m = a'^m$$

所以 a 的象a'为G'的生成元，从而 G'为循环群. 证完.

习　　题

1　证明：a 和a^{-1}是同阶（周期）元素，ab 与 ba也是同阶元素。

2　设 a 的阶为 n，则$a^m = e$，当且仅当$n \mid m$。

3　如果 G只有一个 2 阶元素 a，证明：对于 G的每个元素 x 总有：$xa = ax$。

4　证明：有限群中阶大于 2 的元素的个数一定是偶数。

5　试确定$\{\boldsymbol{Z}_4; +\}$和$\{S_3; \cdot\}$中各元素的阶。

6　证明：循环群是交换群。

7　设 a 的阶为 m，b 的阶为 n，且 $(m, n)=1$，$ab=ba$，则 ab 的阶为 mn。若 $ab\neq ba$，此结论是否成立？

8　证明：若 $ab=ba$，且 a 的阶为2，b 的阶为3，则由 a 和 b 生成的群是循环群，试确定其阶。

9　证明：无限循环群只有两个生成元。

10　设群 G 的元素 a 的阶为 n。证明：a^r 的阶为 $\frac{n}{d}$，这里 $d=(r, n)$ 是 r 和 n 的最大公约数。

11　设 a 是 n 阶循环群 G 的生成元，证明：a^r 是 G 的生成元当且仅当 $(r, n)=1$。

12　试找出 $\mathbf{Z}_{12}$ 的所有生成元，并找出它的所有子群。

13　假定 G 是无限循环群，G' 是任意循环群。证明：$G\sim G'$。

14　设群 $G\cong G'$，则 G 的任一元 a 的阶与 a 的象的阶相同。若 $G\sim G'$，a 和 a 的象的阶是否相同，两者关系如何？

§5　变换群　置换群

这一节我们将讨论两种具体的群——变换群和置换群。从历史上说，群论最初只研究变换群和置换群，以后才讨论抽象群。本节中将给出重要的凯莱（Cayley）定理，指出任何一个抽象群都与变换群同构，任何一个有限群都与置换群同构。

取定一个非空集合 A，用 $T(A)$ 表示集合 A 的全体变换。在第一章§6中已知 $T(A)$ 对变换的乘法做成一个有恒等元的半群，但不做成群。因为，不是每一个变换都有逆变换。今考虑 $T(A)$ 中所有双变换（即可逆变换）做成的子集，记作 $E(A)$，我们有

定理1　$E(A)$ 对变换乘法做成群。

证明　$E(A)$ 满足群的定义。假如 τ_1、τ_2 是 A 的任意两个双变换，由第一章§2的讨论已知 $\tau_1\tau_2$ 也是 A 的双变换。即变换乘法是 $E(A)$ 的代数运算。

（1）变换乘法满足结合律；

（2）恒等变换I_A：$a \longmapsto a$是双变换，显然 I_A是 $E(A)$的恒等元；

（3）每一双变换都是可逆变换，故 $E(A)$中每一元均有逆元。

所以 $E(A)$对变换乘法做成群。证完。

定义　非空集合A的若干个双变换关于变换乘法做成的群，叫做A的一个变换群。

例 1　设A是平面上所有点的集合，平面的绕一个定点的旋转是A的一个双变换，令G是所有绕定点旋转变换做成的集合，则G关于变换乘法做成 $E(A)$的子群。

事实上，如果用τ_θ表示旋转 θ 角的变换，则有

$$\tau_{\theta_1} \cdot \tau_{\theta_2} = \tau_{\theta_1 - \theta_2} \in G$$

G关于变换乘法封闭。对G中任一旋转 τ_θ，有 $\tau_{-\theta} \in G$，显然 $\tau_\theta^{-1} = \tau_{-\theta}$ 即G中每一元素均有逆元。故G是 $E(A)$的子群。称G为**旋转变换群**。

显然G并不包含平面点集合A的所有双变换。因此，除了定理 1 中所说的集合A的所有双变换做成的变换群外，的确还可以由其中一部分双变换做成较小的变换群。

变换群一般不是交换群。

例 2　设τ_1是平面的一个平移，它把原点（0，0）平移到（1，0）。τ_2是绕原点转$\frac{\pi}{2}$的旋转。那么τ_1和 τ_2都是平面点集A的双变换。但

$$(\tau_1\tau_2)(0,0) = \tau_1(\tau_2(0,0)) = \tau_1(0,0) = (1,0)$$

$$(\tau_2\tau_1)(0,0) = \tau_2(\tau_1(0,0)) = \tau_2(1,0) = (0,1)$$

显然，$\tau_1\tau_2 \neq \tau_2\tau_1$。

变换群不仅在数学上，在物理、化学等方面都有广泛的应用，而且在理论上变换群与抽象群之间也有着重要的联系。

定理 2　（凯莱定理）任何一个群都与变换群同构。

证明　设G是一个群，任取其中一元a，利用 a，规定G

的变换如下：

$$\tau_a;\ x\longmapsto ax,\quad \forall x\in G$$

可以验证τ_a是G的一个双变换。因为，$\forall x\in G$，由τ_a可确定G中唯一的一个元ax，所以τ_a是G的一个变换。又因$ax=b$在G中有解，故对G中任意元b，在G中存在一个元x，使$\tau_a(x)=b$，所以τ_a为满变换。又若$x_1\neq x_2$，则$ax_1\neq ax_2$，否则由消去律，由$ax_1=ax_2$，有$x_1=x_2$，与$x_1\neq x_2$矛盾，所以τ_a是单变换，从而τ_a是双变换。

这样对于G中每一元a，按上述办法可得G的一个双变换τ_a，叫做由a确定的左乘变换。

令　$\overline{G}=\{\tau_a|a\in G\}$

下面指出变换的乘法是$\overline{G}$的代数运算。为此只须指出$\overline{G}$中任二元τ_a，τ_b之积仍在$\overline{G}$中即可。$\forall\tau_a,\tau_b\in\overline{G}$

$$\begin{aligned}(\tau_a\cdot\tau_b)(x)&=\tau_a(\tau_b(x))=\tau_a(bx)=a(bx)\\&=(ab)x=\tau_{ab}(x),\quad\forall x\in G\end{aligned}$$

故$\tau_a\tau_b=\tau_{ab}$。由$a,b\in G$，有$ab\in G$，故$\tau_{ab}\in\overline{G}$。所以变换的乘法是$\overline{G}$的代数运算，$\{\overline{G};\ \cdot\}$是一个代数体系。

最后证明：$G\cong\overline{G}$。令

$$\varphi;\ a\longmapsto\tau_a,\quad\forall a\in G$$

显然φ是G到$\overline{G}$的满射。又若$a\neq b$，则必有$ax\neq bx$，于是$\tau_a(x)\neq\tau_b(x)$，即$\tau_a\neq\tau_b$，从而φ是G到$\overline{G}$的单射。故φ是G到$\overline{G}$的双射。

又

$$\varphi(ab)=\tau_{ab}=\tau_a\cdot\tau_b=\varphi(a)\varphi(b)$$

所以φ是G到$\overline{G}$的同构映射，于是$G\cong\overline{G}$。

由§3同构的性质，因G是群知$\overline{G}$也是一个群，且是变换群。这就证明了任一群G同构于G上的一个变换群。证完。

这个定理说明，从同构的意义来讲，任何一个抽象群都可以看做是一个变换群。由此看出变换群在群论中的重要地位。

特别地，当A为n元有限集时，我们称$E(A)$即S_n为n元

置换全体做成的群为 n 次置换群或 n 次对称群。

推论 任何一个有限群都与一个置换群的子群同构。

例 3 $G=\{1,\omega,\omega^2\}$ $(\omega^3=1,\ \omega\neq 1)$。试找出与 G 同构的置换群的子群 $\overline{G}$。

解 利用 G 的元，按照定理 2 中的方法做 τ_a，得

τ_1：$x\longmapsto 1\cdot x$

故

$$\tau_1=\begin{pmatrix}1 & \omega & \omega^2\\ 1 & \omega & \omega^2\end{pmatrix}$$

$$\tau_\omega: x\longmapsto \omega x \quad \tau_\omega=\begin{pmatrix}1 & \omega & \omega^2\\ \omega & \omega^2 & 1\end{pmatrix}$$

$$\tau_{\omega^2}: x\longmapsto \omega^2 x \quad \tau_{\omega^2}=\begin{pmatrix}1 & \omega & \omega^2\\ \omega^2 & 1 & \omega\end{pmatrix}$$

为了书写简明起见，我们把 G 的元素 1，ω，ω^2 分别用 1，2，3 表示。则

$$\tau_1=\begin{pmatrix}1 & \omega & \omega^2\\ 1 & \omega & \omega^2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}=(1)$$

$$\tau_\omega=\begin{pmatrix}1 & \omega & \omega^2\\ \omega & \omega^2 & 1\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=(1\ 2\ 3)$$

$$\tau_{\omega^2}=\begin{pmatrix}1 & \omega & \omega^2\\ \omega^2 & 1 & \omega\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}=(1\ 3\ 2)$$

由 τ_1，τ_ω，τ_{ω^2} 组成的 $\overline{G}=\{(1),(123),(132)\}$。令

$$\begin{aligned}\varphi:\ 1&\longmapsto \tau_1=(1)\\ \omega&\longmapsto \tau_\omega=(123)\\ \omega^2&\longmapsto \tau_{\omega^2}=(132)\end{aligned}$$

于是

$$G\cong\overline{G}\subseteq S_3$$

例 4　设 $G=(a)$ 是 n 阶循环群，则 G 与 S_n 的一个子群 $\overline{G}$ 同构。所以为了找到 $\overline{G}$，只要找出 $\overline{G}$ 的生成元即可。由于生成元的象也是生成元，故只要找出 a 的象即可（见前节命题4）。由凯莱定理的证明知，a 的象为 τ_a，而

$$\tau_a;\ x \longmapsto ax$$

于是有

$$\tau_a=\begin{pmatrix} e & a & a^2 & \cdots & a^{n-1} \\ a & a^2 & a^3 & \cdots & e \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix}$$

$$=(12\cdots n)$$

即 $\overline{G}=((12\cdots n))$。

因例 3 中的 $G=(\omega)$ 是三阶循环群，所以可用例 4 的方法简化例 3 中找同构于 G 的置换群 $\overline{G}$ 的方法。易知 $\overline{G}=((123))$。

由上面的结果可知，每一个有限群都可在置换群中找到一个实例。因为置换群是一种比较容易计算且具体的群，所以通过置换群来研究有限群是非常重要的一种方法。

习　　题

1　假定 $\boldsymbol{R}$ 是所有实数作成的集合，证明：所有 $\boldsymbol{R}$ 的可以写成

$$\varphi_{a,b}:\ x \longmapsto ax+b,\ a,\ b\in \boldsymbol{R},\ a\neq 0$$

形式的变换作成一个变换群。这个群是不是交换群？

2　证明，一个变换群的恒等元一定是恒等变换。

3　试问，由 $(x,\ y)\longmapsto(x+a,\ 0)$ 所定义的平面 π 的所有变换的集合 T，对于变换乘法是否是变换群？

4　试求出与 4 阶群

$$G=\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$$

同构的置换群。

5　证明：第 1 题中的变换群与本章 § 1 习题 2 中的群 G 同构。

§6　子群的陪集

在第一章中我们曾经利用整数 n 把全体整数 $\mathbf{Z}$ 分成剩余类 $\mathbf{Z}_n$。在本章§2中我们又知所有形如$\{kn|k\in\mathbf{Z}\}$的元恰为$\{\mathbf{Z};+\}$的子群$H=(n)$。那么$\mathbf{Z}$的以 n 为模的剩余类$\mathbf{Z}_n$也可以说是利用子群 H 得到的商集，现在我们把这种情形推广，考虑利用一个子群 H 来对群 G 进行分类，并由此得出一些重要结果。

先介绍子集乘积的概念。设G为群，H，K为G的任二子集，G的如下子集

$$\{hk|h\in H,\ k\in K\}$$

叫做子集H与K的乘积，记做 HK。

例 1　$G=S_3$，$H=\{(1),(12),(123)\}$，$K=\{(123),(132)\}$，那么 HK的元素为

$$(1)(123)=(123),\quad (1)(132)=(132)$$
$$(12)(123)=(23),\quad (12)(132)=(13)$$
$$(123)(123)=(132),\quad (123)(132)=(1)$$

故

$$HK=\{(1),(123),(132),(13),(23)\}$$

关于群的三个子集 H_1、H_2、H_3 的乘积，我们有

$$H_1(H_2H_3)=(H_1H_2)H_3$$

这可由群G中元素满足结合律直接得出。上式说明群的子集的乘积也满足结合律。

特别地，当子集H只含一个元素 a 时，即 $H=\{a\}$，则H与K的乘积 HK由形如

$$ak,\ k\in K$$

的元组成。这时就把H与K的乘积记为 aK。这种特殊情况，在今后的讨论中非常重要。

定义 1　假如H是群G的子群，a是 G中任意元，集合 aH (Ha) 叫做G关于子群H的左（右）陪集。

例2　$G=S_3$，$H=\{(1),(12)\}$。已知H是G的子群，按定义1 G关于H的左陪集的做法是，取群G中任一元素从左边去乘H。得到的乘积就是G关于H的一个左陪集。比如，先取元素（1），于是得到左陪集

$$(1)H=\{(1),(12)\}$$

再从$S_3\backslash(1)H$中另取一个元素，比如（13）再做乘积得左陪集

$$(13)H=\{(13),(123)\}$$

然后再从$S_3\backslash(1)H\cup(13)H$中任取一元，比如（23），再做乘积得左陪集

$$(23)H=\{(23),(132)\}$$

于是利用子群H把G的全部元素分做三个子集，即得到G关于子群H的三个左陪集为

$$(1)H,\ (13)H,\ (23)H$$

显然若取元素（12），（123），（132）也可用上法得出同样的三个左陪集

$$(12)H=(1)H,\ (123)H=(13)H,\ (132)H=(23)H$$

令$Q_l=\{(1)H, (13)H, (23)H\}$，显然$Q_l$满足下列三个条件

（i）　$G=S_3=\bigcup\limits_{gH\in Q_l} gH$；

(ii)　若$aH\neq bH$，则$aH\cap bH=\phi$，$\forall a, b\in S_3$；

(iii)　$\forall gH\neq\phi$，$gH\in Q_l$。

由（i）、(ii)、(iii)条说明，用子群H可把S_3分成两两不交的非空子集的并集。即子群H将S_3分成了三个类，而$Q_l=\{(1)H, (13)H, (23)H\}$恰是$S_3$用子群$H$分类所得到的（左）商集。

现在我们来讨论在任意群G中用它的子群H来分类的问题。

命题1　设G为任一群，H为G的一个子群，那么$Q_l=\{gH|g\in G\}$满足

（i） $G=\bigcup\limits_{gH\in Q_l} gH$；

(ii) 若 $aH\neq bH$，则$aH\cap bH=\phi$，$\forall a,b\in G$；

(iii) $\forall gH\neq\phi$，$gH\subset Q_l$。

证明 $\forall g\in G$，显然$g\in gH$，（i）、(iii)成立是明显的。只需证明 (ii)。若$aH\cap bH\neq\phi$，必有元素$x\in aH\cap bH$，于是必存在h_1，$h_2\in H$，使 $x=ah_1=bh_2$，从而 $a=bh_2h_1^{-1}$，于是

$$aH=(bh_2h_1^{-1})H=b(h_2h_1^{-1}H)=bH$$

这说明，G 关于 H的任意两个左陪集或者重合或者没有公共元，(ii) 得证。证完。

命题1 的（i）、(ii)、(iii) 条说明：

$$Q_l=\{gH|g\in G\}$$

是G关于子群H的（左）商集。每一个左陪集gH就是一个类。这样用子群H把群G分成了若干个类。

显然$b\in bH$，若$b\in aH$，那么$aH\cap bH\neq\phi$，由命题1 (ii)的证明，必有$aH=bH$。这就是说，左陪集 aH由其中任一元唯一决定，即与代表的选择无关。一般地，常称 a 为 aH 的代表。

在第一章 § 3 中，我们知道，集合A的一个等价关系决定A的一个商集，反过来，集合A的一个商集也决定A的一个等价关系。现在来看一下用上面办法所得到的G关于子群H的商集决定的等价关系是什么。

首先讨论一下群G的两个元素a，b在H的同一个左陪集（类）中的条件。

假如a，b在H的同一个左陪集中，则有$b=ah$，$h\in H$。因此 $a^{-1}b=h\in H$。反过来，假如 $a^{-1}b\in H$，即 $a^{-1}b=h$，那么$b=ah\in aH$。因此，a，b在同一左陪集中，于是得出：

$$a,\ b\text{ 在 }H\text{ 的同一左陪集（类）中}\Longleftrightarrow a^{-1}b\in H$$

因此，自然地可规定G的元a，b的关系～如下：

$$a\sim b\Longleftrightarrow a^{-1}b\in H$$

这个关系～显然是群G的一个等价关系。由此等价关系所

决定的商集显然就是 Q_l。所以我们也可以先利用子群 H，定义关系～如下

$$a \sim b \Longleftrightarrow a^{-1}b \in H$$

于是得到 G 的一个商集。商集的每个元素（类）就是 G 关于子群 H 的左陪集。因此，H 的左陪集也可以用这种办法来定义。即

由上面的等价关系～所决定的商集的元素（类）叫做群 G 关于子群 H 的左陪集。

上面关于左陪集的讨论完全可以用于右陪集。这时

a，b 在 H 的同一右陪集中 $\Longleftrightarrow ba^{-1} \in H$

或

$$a \sim' b \Longleftrightarrow ba^{-1} \in H$$

一般说来，左陪集不一定等于右陪集，关系～和关系～′也未必相同。

如在例 2 中，$H = \{(1), (12)\}$的右陪集为

$$H(1) = \{(1), (12)\},\ H(13) = \{(13), (132)\}$$

$$H(23) = \{(23), (123)\}$$

由此所得到的（右）商集为

$$Q_r = \{H(1), H(13), H(23)\}$$

显然

$$(13)H \neq H(13),\ (23)H \neq H(23)$$

故

$$Q_l \neq Q_r$$

当群 G 是交换群时，左陪集显然等于右陪集。在一般非交换群中，也可能有那样的子群，它的左陪集和右陪集总是相等的。这样的子群在群的研究中特别重要，在下一节将重点讨论它。

如果 G 是加群，则子群 H 的左陪集 aH 用 $a+H$ 来表示。此时有

$a \sim b$（或 a，b 在 H 的同一左陪集中）$\Longleftrightarrow b-a \in H$

例如，整数加群Z对子群 $H=(4)$来说，有四个陪集：

$$H_0=0+H=H+0=\{\cdots,-12,-8,-4,0,4,8,12,\cdots\}$$

$$H_1=1+H=H+1=\{\cdots-11,-7,-3,1,5,9,13,\cdots\}$$

$$H_2=2+H=H+2=\{\cdots-10,-6,-2,2,6,10,14,\cdots\}$$

$$H_3=3+H=H+3=\{\cdots,-9,-5,-1,3,7,11,15,\cdots\}$$

显然这四个陪集恰好是$\overline{0}$，$\overline{1}$，$\overline{2}$，$\overline{3}$。而a，b在H的同一（左）陪集中，或

$$a\sim b\Longleftrightarrow b-a\in H\ (\text{即}4\,|\,b-a)$$

此时（左）商集

$$Q_l=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$$

从前面例2我们看到一个子群H的左、右陪集并不一定相同，自然左商集与右商集也不一定相等，但是它们所含元素（即陪集）的“个数”却相等。这个结论一般也是对的，因为我们有如下定理。

定理1　群G的子群H的左陪集“个数”和右陪集“个数”相等，即左商集Q_l与右商集Q_r之间存在一个双射。

证明　令

$$\varphi: aH\longmapsto Ha^{-1}$$

下面证明φ是Q_l到Q_r的一个双射。

（1）若$aH=bH$，则有$a^{-1}b\in H$。从而$(a^{-1}b)^{-1}=b^{-1}a\in H$所以有$Ha^{-1}=Hb^{-1}$（由右陪集相等的条件）。

上述说明φ是Q_l到Q_r的映射。

（2）$\forall Ha\in Q_r$：有$a^{-1}H\in Q_l$使

$$\varphi(a^{-1}H)=H(a^{-1})^{-1}=Ha$$

所以φ是一个满射。

（3）若　$\varphi(aH)=\varphi(bH)$，则有　$Ha^{-1}=Hb^{-1}$。从而有$b^{-1}(a^{-1})^{-1}=b^{-1}a\in H$。进一步有　$a^{-1}b=(b^{-1}a)^{-1}\in H$。所以$aH=bH$。

故φ是一个单射。

从而证明了φ是Q_l到Q_r的双射。

由这个定理可知，H有多少个左陪集则H也就有多少个右陪集。于是可以给出

定义 2　群G的子群H的左陪集（或右陪集）的"个数"叫做H在G里的指数，用符号$[G: H]$表示。

一个子群H在G中的指数可以是有限也可以是无限。

例如，取$G=\{Z; +\}$，$H=(n)$，则$[G; H]=n$。对例 2 中的S_3和H来说，$[S_3: H]=3$。

例 3　$G=\{Q; +\}$，H是其中所有偶数构成的子群。H的左陪集为$a+H=\{a+2n \mid a\in Q, n\in Z\}$。则$Q$中任二元$a,b$在$H$的同一左陪集中当且仅当$a-b\in H$。易知对任一奇数 c，

$$c,\ \frac{1}{2}c,\ \cdots,\ \frac{1}{2^n}c,\ \cdots$$

分别在H的不同左陪集中，故$[G; H]$无限。

容易看到，一个群G关于子群H的任二左（右）陪集间还有一个重要联系：

命题 2　**G的子群H与H的每一个左陪集aH之间都存在一个双射。**

证明　令

$$\varphi: h\longmapsto ah$$

则φ是H到aH的一个双射。

因为，H的每一元h都有唯一的象ah，φ是映射；aH的每一元ah都有原象h，φ是满射；若$h_1\neq h_2$时，有$ah_1\neq ah_2$，φ是单射。故φ是H到aH的一个双射。

当G是有限群时，由这个命题立即得到：

定理 2　（拉格朗日（Lagrange）定理）**设G为n阶有限群，H为G的m阶子群，则$m\mid n$。**

证明　因为G的阶n和子群H的阶m都有限，故H在G中的指数j也有限。G的n个元被分成j个左陪集，由命题 2 知每一左陪集皆含m个元，故

$$n=mj,\ 即 m\mid n$$　　证完。

此定理指出了有限群 G 的子群的阶数和群 G 的阶数的关系。n 阶有限群的子群的阶数必是 n 的约数。如 8 阶群绝不会有 3，5，7 阶子群，只可能有 1，2，4，8 阶子群。因此，在找有限群的子群时可去掉一定的盲目性。

定理 3　一个有限群 G 的任一元 a 的阶（周期）m 都整除 G 的阶 n。

证明　由 a 的阶（周期）是 m，则由 a 可生成一个 m 阶子群：$H=\{a^0,a,a^2,\cdots,a^{m-1}\}$，于是由定理 2 可知 $m|n$。

对于 n 阶有限群中任一元 a，显然都有 $a^n=e$。

就例 2 来看，S_3 的阶为 6，子群 H 的阶为 2，H 有三个左陪集，所以 H 的指数为 3。而 2，3 都是 6 的约数，并且

$$6=2\times 3$$

S_3 的 6 个元是：(1)，(12)，(13)，(23)，(123)，(132)。(1) 的阶是 1，(12)，(13)，(23)的阶为 2，(123)，(132)的阶为 3。

又 S_3 为 6 阶群，它的子群的阶只能是 6 的约数。即只能为 1，2，3，6。经过验证知 S_3 恰有下列 6 个子群：

$H_1=\{(1)\}$；$H_2=\{(1),\ (12)\}$；$H_3=\{(1);\ (13)\}$

$H_4=\{(1),\ (23)\}$；$H_5=\{(1),(123),(132)\}$；$H_6=S_3$

习　题

1　设 H 是群 G 的子群。试问，G 关于 H 的所有左陪集中是否有 G 的子群，都是哪些，为什么？

2　$G=\{\mathbf{R};\ +\}$ 是实数加群，$H=\{\mathbf{Z};\ +\}$ 是 G 的子群。试问，G 关于 H 的陪集是由怎样的实数组成的？并指出 H 在 G 中的指数。

3　设 H 是群 G 的子群。a，$b\in G$，证明：以下六个条件是等价的

（1）$b^{-1}a\in H$；（2）$a^{-1}b\in H$；（3）$b\in aH$；

（4）$a\in bH$；（5）$aH=bH$；（6）$aH\cap bH\neq\phi$。

4　证明：阶数是素数 p 的群一定是循环群。

5　设 G 为 n 阶有限群。证明：G 的元素都满足方程

$x^n=e$

6　设H，K是群G的子群。H的阶为m，K的阶为n，且$(m,n)=1$，则$H\cap K=\{e\}$。

7　设群G关于子群H_1与H_2的商集都是有限的。证明：G关于$H_1\cap H_2$的商集也是有限的。

8　证明：S_3是阶数最小的非交换群。

9　设G是6阶群，则G至少含有一个三阶子群。

10　证明：阶数是p^n的群（p是素数）一定包含一个阶数是p的子群。

11　证明：从同构观点看，四阶群只有两个，一个是循环群，一个是克莱茵四元群B_4。

§7　正规子群与商群

在上节例2中我们看到，一个群G的子群H的左、右陪集aH与Ha不一定相等，由H所决定的两个商集Q_l，Q_r也不一定相等。但对例2中的S_3来说，若取S_3的子群为$K=\{(1),(123),(132)\}$时，则由子群K所决定的左陪集为

$$(1)K=\{(1),(123),(132)\}$$

$$(12)K=\{(12),(23),(13)\}$$

于是由K决定的左商集为

$$Q_l=\{(1)K,(12)K\}$$

而K的右陪集为

$$K(1)=\{(1),(123),(132)\}$$

$$K(12)=\{(12),(13),(23)\}$$

于是有

$$(1)K=K(1),\quad (12)K=K(12)$$

这说明，子群K的每一个左陪集也是一个右陪集，即$aK=Ka$对任意$a\in G$均成立。于是左、右商集相等$Q_l=Q_r$。具有此种特性的子群，在群论的研究中起着特别重要的作用，本节将重点讨论之。

定义　设N是群G的一个子群，如果

$$aN=Na \qquad \forall a\in G$$

则称N是G的一个正规子群（或不变子群）。

上面提到的S_3中的子群K就是S_3的一个正规子群，而 $H=\{(1),(12)\}$不是S_3的正规子群。

由定义，对正规子群N没有区分左、右陪集的必要，而简称为N的陪集。左、右商集是同一集合，今后统一地记作G/N。

例 1　任意群G的平凡子群G和$\{e\}$都是G的正规子群。因为$\forall a\in G$，$Ga=aG=G$，$ea=ae=a$。且$G/G=\{G\}$，$G/\{e\}=G$（以后约定陪集$a\{e\}$记作 ae）。

例 2　交换群G的每一个子群H显然都是正规子群。

例 3　群G的中心（见本章§2习题1）

$$C(G)=\{x\,|\,x\in G \quad xa=ax \quad \forall a\in G\}$$

是G的正规子群。

解　已知$C(G)$是G的子群，只须证明$C(G)$是G的正规子群。因为G的每一元a和$C(G)$的每一元x可交换，显然$aC(G)=C(G)a$，故$C(G)$是G的正规子群。

例 4　设H是G的子群，且H在G中的指数为2，则H是G的正规子群。

证明　$\forall a\in G$,若$a\in H$,则$aH=H=Ha$。若 $a\bar{\in} H$，则H，aH是G的两个不同的左陪集，由$[G:H]=2$，故$G=H\cup aH$，同理$G=H\cup Ha$，又$H\cap aH=\phi=H\cap Ha$，故 $aH=G\backslash H=Ha$，即对于任意$a\in G$，均有 $aH=Ha$，故H为G的正规子群。

为了便于检验一个子群是否是正规子群，再给出几个等价条件。

定理　设N是群G的子群，下面四个条件是等价的。

（1）N是G的正规子群；

（2）$aNa^{-1}=N$，$\forall a\in G$；

（3）$aNa^{-1}\subseteq N$，$\forall a\in G$；

（4）$ana^{-1}\in N$，$\forall a\in G$，$\forall n\in N$。

证明 按照下列途径：（1）⇒（2）⇒（3）⇒（4）⇒（1）来证明定理成立。

（1）⇒（2）因N是正规子群，$\forall a\in G$，有 $aN=Na$．于是 $aNa^{-1}=(aN)a^{-1}=(Na)a^{-1}=Naa^{-1}=Ne=N$．即（2）成立。

（2）⇒（3） $\forall a\in G$，$aNa^{-1}=N$，显然 $aNa^{-1}\subseteq N$。

（3）⇒（4） 由$aNa^{-1}\subseteq N$，$\forall a\in G$，$\forall n\in N$，都有$ana^{-1}\in N$。

（4）⇒（1） $\forall an\in aN$，$a\in G,n\in N$，由（4）$ana^{-1}\in N$，故存在 $n_1\in N$，使 $ana^{-1}=n_1$，即 $an=n_1a$，从而 $an\in Na$，故 $aN\subseteq Na$。另一方面，$\forall na\in Na$，由 $a^{-1}na\in N$（将（4）中的 a 换成a^{-1}即得）故存在$n_2\in N$，使 $a^{-1}na=n_2$，从而 $na=an_2\in aN$，故$Na\subseteq aN$。因此

$$aN=Na,\quad \forall a\in G$$

故N是G的正规子群．证完。

这个定理说明，判断一个子群N是否是正规子群，可以用（1）、（2）、（3）、（4）中任何一条．一般来说用条件（4）比较方便，因为这个条件只需验证ana^{-1}是否在N中，而不需要判断两个子集是否相等。

例 5 群$GL_n(R)=\{(a_{ij})\,|\,|a_{ij}|\neq 0\}$，

$SL_n(R)=\{(a_{ij})\,|\,|a_{ij}|=1\}$，$H=\{(a_{ij})\,|\,a_{ij}=0,\ i\neq j$，且$|a_{ij}|\neq 0\}$

已知$SL_n(R)$是$GL_n(R)$的子群（见本章§2例3），下面证明$SL_n(R)$是$GL_n(R)$的正规子群。

$$\forall A\in GL_n(R),\ B\in SL_n(R)，因为$$

$$|ABA^{-1}|=|A|\cdot|B|\cdot|A^{-1}|=|B|=1$$

故

$$ABA^{-1}\in SL_n(R)$$

所以$SL_n(R)$是$GL_n(R)$的正规子群。

显然H是 $GL_n(R)$ 的子群，但不是正规子群．事实上，若取

$$h=\begin{pmatrix}1 & & & \\ -1 & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix},\quad a=\begin{pmatrix}1 & 1 & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}\in GL_n(\boldsymbol{R})$$

则有

$$aha^{-1}=\begin{pmatrix}1 & 1 & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}\cdot\begin{pmatrix}1 & & & \\ & -1 & & \\ & & 1 & \\ & & & \ddots & \\ & & & & 1\end{pmatrix}\begin{pmatrix}1 & 1 & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}^{-1}$$

$$=\begin{pmatrix}1 & 2 & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}\overline{\in} H$$

所以H不是 $GL_n(\boldsymbol{R})$的正规子群。

下面讨论由群G对正规子群N所决定的商集$G/N=\{aN, bN, \cdots\}$。

我们已经看到剩余类加群 $\boldsymbol{Z}_n$ 就是按剩余类的加法

$$\overline{i}+\overline{j}=\overline{i+j}$$

作成的一个群，而$\boldsymbol{Z}_n$正是整数加群$\boldsymbol{Z}$对正规子群$H=(n)$所决定的商集.

对于群G的任一正规子群N所决定的商集

$$G/N=\{aN, bN, cN, \cdots\}$$

能否如 $\boldsymbol{Z}_n$一样，自然地规定一种运算，使之成为群呢？

首先得看一看对于G/N中任二元素（左陪集）aN，bN能否自然地引进运算，即从两个左陪集得到G/N中唯一的一个左陪集。

显然aN，bN对G/N来说是G/N的元素，对G来说是G的子集，把aN，bN做为G的子集相乘，其结果得到G的一个子集

$$aN\cdot bN=aNbN$$

因为左陪集必须是形如gN的子集，所以一般来说，这个子集

$aNbN$ 未必是一个左陪集．但对于正规子群N来说，N的任意两个左陪集aN，bN 的乘积

$$aN\cdot bN=aNbN=ab\cdot NN=abN\ (\text{因}NN=N)$$

仍是一个左陪集．且 aN，bN的积与代表的选择无关，是唯一确定的．这是因为

若$aN=a'N$，$bN=b'N$，那么$a=a'n_1$，$b=b'n_2$,其中$n_1,n_2\in N$．于是$ab=a'n_1b'n_2$．由于N是正规子群,所以 $n_1b'\in Nb'=b'N$．于是存在$n_3\in N$，使 $n_1b'=b'n_3$．这时，$ab=a'b'n_3n_2=a'b'(n_3n_2)\in a'b'N$．故有 $abN=a'b'N$．

这说明，当N为正规子群时，子集的乘积

$$aN\cdot bN=abN$$

是商集G/N的一个代数运算，$\{G/N;\ \cdot\}$是一个代数体系．

下面再看一看，G/N按上述规定的乘法是否构成群．这只要逐条验证群的条件就可以了．

（1）因为G/N的代数运算是由G的代数运算确定的，而G的运算满足结合律，所以G/N的运算也满足结合律；

（2）$(eN)(aN)=(ea)N=aN$，所以 $eN=N$为G/N 的恒等元；

（2）$\forall aN\in G/N$，$a\in G$，而 G是群，故有 $a^{-1}\in G$，$a^{-1}N\in G/N$ 满足条件：$(aN)\ (a^{-1}N)=(aa^{-1})N=eN=N$，即$G/N$中任意元都有逆元．

综合上述可知$\{G/N;\ \cdot\}$是群，称为G关于正规子群N的商群．

因为N在G中的指数〔G：N〕就是N的陪集的个数，亦即商群的阶．故当G为有限群时，由拉格朗日定理有

$$\frac{G\text{的阶}}{N\text{的阶}}=G/N\text{的阶}$$

例 6　$G=S_3$，子群 $K=\{(1),(123),(132)\}$，已知K是S_3的正规子群，K的指数为 2，商群 $G/K=\{(1)K,(12)K\}$为二元群，其运算表为

$\cdot$	$(1)K$	$(12)K$
$(1)K$	$(1)K$	$(12)K$
$(12)K$	$(12)K$	$(1)K$

显然$(1)K=K$为 G/K 的恒等元，每一元素的逆元是自身。

例 7　设 $G=\{Q;\ +\}$，$H=\{Z;\ +\}$；显然 H是G的子群。因G为交换群，故H为G 的正规子群。$\forall a\in G$，a 所在的陪集为$a+H=\{a+k|k\in Z\}$，例如，$\frac{1}{3}$所在的陪集为$\frac{1}{3}+H$

$=\{\cdots,\ \frac{1}{3}+(-n),\cdots,\ \frac{1}{3}+(-1),\frac{1}{3},\ \frac{1}{3}+1,\cdots,\ \frac{1}{3}+n,$

$\cdots\}$。

由于$a+H=b+H\Longleftrightarrow b-a\in H$，这一事实表明$\frac{1}{3}+H\neq\frac{2}{3}$

$+H$，而$\frac{1}{3}+H=\frac{4}{3}+H$。由于不同的正既约真分数(即 0 与 1 之间的既约分数）之差不可能是整数，所以它们所在的陪集不同，并且任一非整数的有理数，均含在某一以正既约真分数为代表的陪集中，故商群

$$G/H=\left\{H,\ \frac{1}{2}+H,\ \frac{1}{3}+H,\ \frac{2}{3}+H,\ \frac{1}{4}+H,\right.$$

$$\frac{3}{4}+H,\ \frac{1}{5}+H,\ \frac{2}{5}+H,\ \frac{3}{5}+H,\ \frac{4}{5}+H,\ \frac{1}{6}+H,\ \frac{5}{6}+$$

$$\left.H,\ \cdots\right\}$$

为无限群。

G/H的运算为：$(a+H)+(b+H)=(a+b)+H$

例如，$\left(\frac{2}{3}+H\right)+\left(\frac{1}{4}+H\right)=\frac{11}{12}+H$

$$\left(\frac{2}{3}+H\right)+\left(\frac{5}{6}+H\right)=\frac{9}{6}+H=\frac{1}{2}+H$$

H是 G/H的零元，$a+H$ 的负元是$(-a)+H$。

对任意$\frac{q}{p}+H\in G/H$，$p\left(\frac{q}{p}+H\right)=H$。故$G/H$中每一元的阶（周期）都有限。我们已知有限群的元素的阶（周期）必定是有限的。此例说明，每一元素的阶都有限的群不一定是有限群。

习　　题

1　证明：两个正规子群的交是正规子群。

2　证明：群G的 2 阶正规子群必含在G的中心里。

3　证明：G的子群H是正规子群的充要条件是：$G=N(H)$（$N(H)$为H的正规化子，见§ 2 习题 2）。

4　若群G的子群H 的任意两个左陪集的乘积仍是一个左陪集，则H是G的正规子群。

5　若H是群G的 仅有的n阶子群（即G只有一个n阶子群），则H是G的正规子群。

6　设A，B是群G的子群，且A是正规子群，则 AB是G的子群。

7　设A，B都是群G的正规子群，证明：AB 也是G的正规子群。

8　设H_i（$i=1,2,\cdots$）是群G的正规子群，并且

$H_1\subseteq H_2\subseteq H_3\subseteq\cdots\subseteq H_n\subseteq\cdots$

则

$$H=\bigcup_{i=1}^{\infty}H_i$$

是G的正规子群。

9　举例说明群G的正规子群 N的正规子群 K未必是 G的正规子群。

10　设H是含于群G的中心的子群，则H是G的正规子群。若G/H是循环群，则G是交换群。

11　一个群G的可以写成$aba^{-1}b^{-1}=[a,b]$形式的元叫做换位子。证明：

（1）G的一切有限个换位子的乘积作成的集合C是G的一个正规子群；

（2）G/C是交换群；

（3）若N是G的一个正规子群，并且G/N为交换群，则$N\supseteq C$。

12 设G为有限交换群，G的阶为n，p为素数且$p|n$。证明：G中存在阶为p的元素。

13 如果群G除平凡子群外无其它正规子群时，称G为单群。证明：有限交换群G是单群的充分必要条件是G的阶是素数。

§8 群的同态基本定理

在§3中我们讨论了群的同构和同态的概念。上节又给出了正规子群与商群的概念。本节讨论群G和正规子群N及其共同决定的商群G/N与G的同态象之间的密切关系。给出群的同态基本定理，这是群论中重要结果之一。

为了下面讨论方便，先给出

命题 假定φ是群G到群G'的满同态。那么G'的恒等元e'在G中的完全原象$N=\{x|x\in G,\ \varphi(x)=e'\}$是$G$的正规子群。称$N$为同态映射$\varphi$的核，记作$\ker\varphi$。

证明 先证N是G的子群。$\forall a,\ b\in N$。由于$\varphi(a)=e'$，$\varphi(b)=e'$，因此

$$\varphi(ab^{-1})=\varphi(a)\varphi(b^{-1})=\varphi(a)\varphi(b)^{-1}=e'\cdot e'^{-1}=e'$$

故

$$ab^{-1}\in N$$

所以N是G的一个子群。

再证N是G的正规子群。$\forall\ n\in N,\ a\in G$，在φ之下看ana^{-1}的象

$$\varphi(ana^{-1})=\varphi(a)\varphi(n)\varphi(a^{-1})=\varphi(a)e'\varphi(a)^{-1}=e'$$

故$ana^{-1}\in N$。所以N是G的正规子群，证完。

现在来讨论群G和它的任一商群G/N的关系。

定理1 设G为群，N为G的任一正规子群，则G与它的

商群G/N满同态，其同态核为N。

证明 要证G与G/N满同态，必须给出G到G/N的一个满射ν，证明ν保持运算，即ν是同态映射。再证ν的核为N即可。

对于G的每一元a，自然地可唯一决定G/N的一个元素，即a所在的陪集 aN。规定

$$\nu: a \longmapsto aN$$

显然ν是G到G/N的满射。

下证ν保持运算。$\forall a,b \in G$，则有

$$\nu: a \longmapsto aN, \quad b \longmapsto bN$$

$$ab \longmapsto (ab)N = (aN)\cdot(bN)$$

即 $$\nu(ab) = \nu(a)\cdot\nu(b)$$

故

$$G \overset{\nu}{\sim} G/N$$

称ν为G到G/N的自然同态。

最后指出ν的核为N。因为N是商群的恒等元，$\forall n \in N$，则$\nu(n) = nN = N$。即$N \subseteq \ker\nu$。反之，$\forall x \in \ker\nu$，即$\nu(x) = xN = N$，从而$x \in N$，即$\ker\nu \subseteq N$。故N恰为ν之核。证完。

定理2 假设φ是群G到G'的满同态，其核为N，则

$$G/N \cong G'$$

证明 要证G/N与G'同构，必须给出一个G/N到G'的双射$\overline{\varphi}$，并证$\overline{\varphi}$保持运算，这里的关键是怎样确定$\overline{\varphi}$。对于G/N中任一元aN，其代表元a在φ之下对应G'中唯一的元素$a' = \varphi(a)$。所以可以借助aN的代表元a在φ之下的象$\varphi(a)$去规定aN的象，于是可规定

$$\overline{\varphi}: aN \longmapsto a' = \varphi(a)$$

但aN中任一元均可做为其代表元，会不会由于代表元选择的不同而使其象也不同呢？这就产生了一个这种规定是否合理的问题。因此，还必须证明此种规定和代表元的选取无关。

若 $aN=bN$，则存在 $n\in N$，使$a=bn$，于是

$$\varphi(a)=\varphi(bn)=\varphi(b)\varphi(n)=\varphi(b)e'=\varphi(b)$$

故

$$\overline{\varphi}(aN)=\overline{\varphi}(bN)$$

这说明，在$\overline{\varphi}$之下G/N的每一个元素在 G' 中有唯一的象，即$\overline{\varphi}$是G/N 到 G' 的一个映射．

下面来证明$\overline{\varphi}$是 G/N到 G' 的双射．

（1）$\forall a'\in G'$，因φ是G到 G'的满射，故在G中至少有一个元素 a，使$\varphi(a)=a'$．由$\overline{\varphi}$的定义知，有 $aN\in G/N$，使

$$\overline{\varphi}(aN)=a'$$

故$\overline{\varphi}$是G/N到G' 的满射．

（2）若$aN=bN$，则有$a^{-1}b\in N$，于是

$$\varphi(a^{-1}b)=\varphi(a^{-1})\varphi(b)=\varphi(a)^{-1}\varphi(b)=e'$$

故有，$\varphi(a)=\varphi(b)$，即$\overline{\varphi}$是单射．

（1）与（2）说明$\overline{\varphi}$是 G/N到 G' 的双射．

最后证明$\overline{\varphi}$保持运算．

任取aN，$bN\in G/N$，则

$$\overline{\varphi}(aN\cdot bN)=\overline{\varphi}(abN)=\varphi(ab)=\varphi(a)\varphi(b)$$
$$=\overline{\varphi}(aN)\cdot\overline{\varphi}(bN)$$

故$\overline{\varphi}$是同构映射，于是

$$G/N\cong G'$$

证完．

定理1、定理2统称为群的同态基本定理．定理1说明：一个群G的任一商群均是G的同态象；定理2说明：G的任一同态象从代数观点看，只能是它的商群．所以，可以认为定理2是定理1的逆定理．由G的任一正规子群都能得到G的一个同态象，反之也对．因此，用正规子群能够决定 G 的所有同态象．另外，我们知道，G的同态象 G' 的性质与G的性质并不完全一样，但定理2告诉我们，在G中一定有一个正规子群N（即同态的核）使得 G' 的性质与商群 G/N 的完全一样．因

此，只要掌握了G/N，即掌握了 G'。从这里使我们看到正规子群和商群的重要意义。群的同态基本定理是群论中最重要的定理之一，许多涉及群的同构或同态的问题都要用到它，读者必须很好掌握。

例 1　设$G=GL_n(R)$，$G'=\{\dot{R};\ \cdot\}$，在本章 § 3 习题 2 中已证，在映射

$$\varphi:\ (a_{ij})\longmapsto |a_{ij}|$$

之下$G\sim G'$。今求出φ的核。由于$G'=\{\dot{R};\ \cdot\}$的恒等元为 1，故φ的核是$GL_n(R)$中所有行列式等于 1 的n阶方阵，即$\varphi^{-1}(1)=SL_n(R)$。于是由定理 2 知

$$GL_n(R)/SL_n(R)\cong\dot{R}$$

例 2　$G=\mathbf{Z}_{12}$（加群），$G'=\{1,-1,i,-i\}$（乘群）在映射φ：

$$\begin{array}{cccc}
\overline{0}\searrow & \overline{1}\searrow & \overline{2}\searrow & \overline{3}\searrow \\
\overline{4}\longmapsto 1, & \overline{5}\longmapsto i, & \overline{6}\longmapsto -1, & \overline{7}\longmapsto -i \\
\overline{8}\nearrow & \overline{9}\nearrow & \overline{10}\nearrow & \overline{11}\nearrow
\end{array}$$

之下G与G'同态（请读者自证）。其核为 $N=\{\overline{0},\ \overline{4},\ \overline{8}\}$。显然$N$为$G$的正规子群。

商群 G/N：N，$\overline{1}+N$，$\overline{2}+N$，$\overline{3}+N$。

规定

$$\begin{aligned}
\overline{\varphi}:\ N&\longmapsto\varphi(\overline{0})=1\\
\overline{1}+N&\longmapsto\varphi(\overline{1})=i\\
\overline{2}+N&\longmapsto\varphi(\overline{2})=-1\\
\overline{3}+N&\longmapsto\varphi(\overline{3})=-i
\end{aligned}$$

显然$\overline{\varphi}$为G/N到G'的双射，且

$$\overline{\varphi}((\overline{a}+N)+(\overline{b}+N))=\overline{\varphi}((\overline{a}+\overline{b})+N)=\varphi(\overline{a}+\overline{b})=\varphi(\overline{a})\varphi(\overline{b})=\overline{\varphi}(\overline{a}+N)\cdot\overline{\varphi}(\overline{b}+N)$$

故$\overline{\varphi}$是G/N到G'的同构映射．即$G/N\cong G'$．

（显然 $G/N=(\overline{1}+N)$ 为 4 阶循环群，$G'=(i)$ 也为 4 阶循环群，由 § 4 循环群的结构定理知 $G/N\cong G'$．）

例 3 设φ是G到 G'的满同态，N'是 G' 的正规子群，$N=\varphi^{-1}(N')=\{a\in G\mid\varphi(a)\in N'\}$，证明：$N$是$G$的正规子群，并且

$$G/N\cong G'/N'$$

证明 证明的基本思路是，如果能证明$G\sim G'/N'$，且同态核为N，则由命题知，N为G的正规子群，再由定理 2 即得$G/N\cong G'/N'$．

先证$G\sim G'/N'$．已知$G\overset{\varphi}{\sim}G'$，又由定理 1 知，$G'\overset{\nu}{\sim}G'/N'$为自然同态，即 $\nu(a')=a'N'$．取 $\overline{\varphi}=\nu\varphi$．可证$\overline{\varphi}$是$G$到$G'/N'$的一个满同态．因为，$G\overset{\varphi}{\sim}G'\overset{\nu}{\sim}G'/N'$，由于$\varphi$，$\nu$都是满射，所以$\overline{\varphi}=\nu\varphi$也是$G$到$G'/N'$的满射．又 $\forall a,b\in G$，有

$$\begin{aligned}\overline{\varphi}(ab)&=(\nu\varphi)(ab)=\nu(\varphi(ab))=\nu(\varphi(a)\varphi(b))\\&=\nu(\varphi(a))\cdot\nu(\varphi(b))=(\nu\varphi)(a)\cdot(\nu\varphi)(b)\\&=\overline{\varphi}(a)\cdot\overline{\varphi}(b)\end{aligned}$$

故$\overline{\varphi}$是G到G'/N'的一个满同态，从而 $G\sim G'/N'$．

再证 $\ker\overline{\varphi}=N$．$\forall a\in N$，则$\varphi(a)\in N'$，从而 $\varphi(a)N'=N'$．于是

$$\overline{\varphi}(a)=(\nu\varphi)(a)=\nu(\varphi(a))=\varphi(a)N'=N'$$

因为N'为G'/N'的恒等元，故$a\in\ker\overline{\varphi}$．即$N\subseteq\ker\overline{\varphi}$．

反之，$\forall a\in\ker\overline{\varphi}$，即$\overline{\varphi}(a)=N'$．但

$$\overline{\varphi}(a)=(\nu\varphi)(a)=\nu(\varphi(a))=\varphi(a)N'=N'$$

故$\varphi(a)\in N'$．因此$a\in N$．从而 $\ker\overline{\varphi}\subseteq N$．故$N=\ker\overline{\varphi}$．

由命题知N为G的正规子群，再由定理 2 知

$$G/N\cong G'/N'$$

习　　题

1　G是可换群，k是取定的正整数，令

$$\varphi: a \longmapsto a^k$$

证明φ是G的自同态，找出$\text{im}\varphi$和$\ker\varphi$。

2　设$G \overset{\varphi}{\sim} G'$，同态核为$N=\varphi^{-1}(e')$。证明：$G$ 中任意两个元素a，b在G'中有相同的象的充要条件是，a,b 在N的同一陪集中。

3　设$G \overset{\varphi}{\sim} G'$，$\ker\varphi=K$。$H$是群$G$的子群。证明：$\varphi^{-1}(\varphi(H))=HK$。当$H\supseteq K$时，有 $\varphi^{-1}(\varphi(H))=H$。

4　设φ是G到 G'的满同态。证明：φ是群G到群G'的同构映射的充要条件是，其核$\varphi^{-1}(e')=\{e\}$。这里e,e'分别是G和G'的恒等元。

5　设φ是群G_1到群G_2的满同态。证明：

（1）若H_1是G_1的正规子群，则$\varphi(H_1)$是 G_2的正规子群；

（2）若H_2是G_2的正规子群，则$\varphi^{-1}(H_2)$是G_1的正规子群。

6　证明：单群（定义见本章§7习题13）的同态象是单群或恒等元群。

7　试决定以12为模的剩余类加群 $\boldsymbol{Z}_{12}$和3次对称群 S_3 的所有同态象。

8　设G_1与G_2分别是n_1与n_2 阶循环群。证明：$G_1\sim G_2$ 当且仅当$n_2|n_1$。

9　设φ是群G到群G'的满同态，$\ker\varphi=K$。令$A=\{H|H$是G的子群，且$H\supseteq K\}$，A'是G'的所有子群的集合，证明

$$\varphi: H\longmapsto\varphi(H)$$

是A到A'的双射。当且仅当H是G的正规子群时，$\varphi(H)$是 G'的正规子群。

10　证明：G/N的任一子群是H/N，其中H是群G的子群，且 $H\supseteq N$。

11　设K，N是群G的两个正规子群，并且 $K\supseteq N$。证明：K/N 是G/N的正规子群，并且

$$(G/N)\Big/(K/N)\cong G/K$$

12　设 K，N 是G的两个正规子群，则

$$(G/N)\Big/(KN/N)\cong G/KN$$

13 用同态基本定理证明循环群$G=(a)$的结构定理，即

1）当a的阶无限时，则$(a)\cong\{\mathbf{Z};\ +\}$

2）当a的阶为n时，则$(a)\cong\{\mathbf{Z}_n;\ +\}$

14 设N是群G的阶为n的正规子群，N在G中的指数为m，且$(m,n)=1$。证明：N是G的唯一的一个阶数为n的子群。

§9 直　　和

在研究代数体系的结构时，常将几个群合成，从而构造一个新的群，也常将一个群分解成几个构造比较简单的群来研究。这是近世代数中处理问题的基本方法。对于加群来说，直和是其主要的合成和分解的手段，在讨论群的构造时起着重要作用。本节主要介绍“直和”的基本概念和基本性质。

定义1 设$\{G_i;\ +\}(i=1,2,\cdots,n)$是$n$个加群。$G=\{(a_1,a_2,\cdots,a_n)\,|\,a_i\in G_i,i=1,2,\cdots,n\}$是$G_1,G_2,\cdots,G_n$的笛卡尔积。$\forall\alpha=(a_1,a_2,\cdots,a_n)$，$\beta=(b_1,b_2,\cdots,b_n)\in G$。规定加法为

$$\alpha+\beta=(a_1+b_1,a_2+b_2,\cdots,a_n+b_n)$$

显然$\{G;\ +\}$是群。称$\{G;\ +\}$为群$\{G_i;\ +\}$ $(i=1,2,\cdots,n)$的（外）直和。记作

$$G=G_1\oplus G_2\oplus\cdots\oplus G_n$$

例1 设$\{\boldsymbol{R};\ +\}$，是实数加群，

$$G=\{(a,\ b)\,|\,a,\ b\in\boldsymbol{R}\}$$

$\forall(a_1,b_1),(a_2,b_2)\in G$，规定加法为

$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$$

显然G是群。$G=\boldsymbol{R}\oplus\boldsymbol{R}$

例2 设$\{\boldsymbol{R};\ +\}$是实数加群，$\{\mathbf{Z};\ +\}$是整数加群，

$$G=\{(a,n)\,|\,a\in\boldsymbol{R},n\in\mathbf{Z}\}$$

$\forall(a,n)$，$(b,m)\in G$，规定加法为

$$(a,n)+(b,m)=(a+b,n+m)$$

则G是群。$G=R\oplus \mathbf{Z}$。

例 3　设$\{\mathbf{Z};\ +\}$是整数加群，$\{\mathbf{Z}_6;\ +\}$是以 6 为模剩余类加群，

$$G=\{(a,\ \overline{b})\mid a\in \mathbf{Z},\ \overline{b}\in \mathbf{Z}_6\}$$

$\forall (a,\ \overline{b})$，$(c,\ \overline{d})\in G$，规定加法为

$$(a,\ \overline{b})+(c,\ \overline{d})=(a+c,\ \overline{b+d})$$

则G是群，$G=\mathbf{Z}\oplus \mathbf{Z}_6$

由以上三例我们可以看到（外）直和的具体构造方法，以及如何依据所给群的运算来规定（外）直和的运算。这几个例子还说明所给的群可以相同也可以不同。

下面的定理给出（外）直和的基本性质。

定理　设$G=G_1\oplus G_2\oplus\cdots\oplus G_n$，则

（1）$\overline{G}_i=\{(0,\cdots,0,a_i,0,\cdots,0)\in G\mid a_i\in G_i\}$

是G的子群，在映射

$$\varphi:\ a_i\longmapsto (0,\cdots,0,a_i,0\cdots,0)$$

之下，有 $G_i\cong \overline{G}_i$。

（2）$\forall (a_1,a_2,\cdots,a_n)\in G$，皆可表为

$$(a_1,a_2,\cdots,a_n)=(a_1,0,\cdots,0)+(0,a_2,\cdots,0)+\cdots+(0,0,\cdots,a_n)$$

其中$(0,\cdots0,a_i,0,\cdots,0)\in \overline{G}_i\ (i=1,2,\cdots,n)$，且表法唯一。

此定理留给读者自证。

定义 2　设$\{G;\ +\}$是加群，$G_i\ (i=1,2,\cdots,n)$ 是G的n个子群，则

$$G_1+G_2+\cdots+G_n=\{a_1+a_2+\cdots+a_n\in G\mid a_i\in G_i\}$$

构成G的子群，称此子群为子群$G_1,G_2,\cdots,G_n$的和。如果

$$G=G_1+G_2+\cdots+G_n$$

则说群G分解成子群$G_1,G_2,\cdots,G_n$的和。

例 4　设$\mathbf{Z}_6$是以 6 为模的剩余类加群。$G_1=\{\overline{0},\ \overline{3}\}$，$G_2=\{\overline{0},\ \overline{2},\ \overline{4}\}$是$\mathbf{Z}_6$的两个子群。于是有

$G_1+G_2=\{\overline{0}+\overline{0}=\overline{0},\overline{0}+\overline{2}=\overline{2},\overline{0}+\overline{4}=\overline{4},\ \overline{3}+\overline{0}=\overline{3},\ \overline{3}+\overline{2}=\overline{5},\ \overline{3}+\overline{4}=\overline{1}\}=\mathbf{Z}_6$

故可说：G分解成子群G_1与G_2的和。

例 5 设 $G=R\oplus R$，R是实数加群，令

$$G_1=\{(m,n)\in G\mid m,n\in\mathbf{Z}\}$$
$$G_2=\{(a,0)\in G\mid a\in R\}$$
$$G_2=\{(0,l)\in G\mid l\in\mathbf{Z}\}$$

则 G_1，G_2，G_3 是G的三个子群，且有

$G_1+G_2+G_3=\{(m,n)+(a,0)+(0,l)=(m+a,n+l)\mid a\in R,m,n,l\in\mathbf{Z}\}=\{(b,k)\mid b\in R,\cdot k\in\mathbf{Z}\}\subset G$。此时 G_1,G_2,G_3之和显然是G的真子群，G不能分解成 G_1,G_2,G_3 之和。

定义 3 设 $G=G_1+G_2+\cdots+G_n$ 为加群G关于子群 G_i $(i=1,2,\cdots,n)$的一个和的分解式。如果G中元素表成 G_i $(i=1,2,\cdots,n)$ 中元素之和时，表法唯一，则称此和为(内)直和。此时称G分解为子群G_i $(i=1,2,\cdots,n)$ 的（内）直和，记为

$$G=G_1\oplus G_2\oplus\cdots\oplus G_n$$

例 6 设$G=R\oplus R$，R是实数加群，令

$$H_1=\{(a,n)\mid a\in R,n\in\mathbf{Z}\}$$
$$H_2=\{(0,b)\mid b\in R\}$$

则H_1，H_2是G的子群，且

$$H_1+H_2=\{(a,n)+(0,b)=(a,n+b)\mid a,b\in R,\ n\in\mathbf{Z}\}$$
$$=\{(a,c)\mid a,c\in R\}=G$$

故知G可分解为子群H_1与H_2之和，又若 $(a,b)\in G=H_1+H_2$，则

$$(a,b)=(a,n)+(0,b-n)$$

$\forall n\in\mathbf{Z}$皆成立。于是，G中元素(a,b)表成 H_1与 H_2元素之和时，表法不唯一，故此和不是直和。

例 7 设$G=R\oplus R$，R为实数加群，令

$$\overline{G_1}=\{(a,0)\mid a\in R\}$$
$$\overline{G_2}=\{(0,b)\mid b\in R\}$$

则$\overline{G_1}$与$\overline{G_2}$为G的子群，且有

$$\overline{G_1}+\overline{G_2}=\{(a,0)+(0,b)=(a,b)\mid a,b\in R\}=G$$

故知G可分解成$\overline{G_1}$与$\overline{G_2}$之和，且若

$$(a,b)=(x_1,x_2)+(y_1,y_2)$$

$(x_1,x_2)\in\overline{G_1}$，$(y_1,y_2)\in\overline{G_2}$是$(a,b)$分解成$\overline{G_1}$与$\overline{G_2}$中元素之和时，则$x_2=y_1=0$，于是有

$$(a,b)=(x_1,0)+(0,y_2)=(x_1,y_2)$$

故有$x_1=a$，$y_2=b$，即

$$(a,b)=(a,0)+(0,b)$$

(a, b)的表法是唯一确定的，于是知 $G=\overline{G_1}\oplus\overline{G_2}$。

习　　题

1　证明：加群G分解成子群G_1与G_2之和为（内）直和必要且只要G_1与G_2的交是零子群。

2　设$G_1=\{\overline{0},\ \overline{3}\}$，$G_2=\{\overline{0},\ \overline{2},\ \overline{4}\}$是加群$\mathbf{Z}_6$的两个子群。试做$G_1$与$G_2$的（外）直和，并证明它同构于$G_1$与$G_2$的（内）直和。

3　对于加群G_1,G_2的(外)直和$G_1\oplus G_2$，证明：$G_1\cong G\oplus G_2/\overline{G_2}$。其中 $\overline{G_2}=\{(0,b)\mid b\in G_2\}$是$G_1\oplus G_2$的子群。

4　令$G_1\oplus G_2$是G的子群G_1与G_2的（内）直和，证明：$G_1\cong G_1\oplus G_2/G_2$。

第三章　环　与　域

在第二章讨论了有一个代数运算的代数体系——群，本章将讨论有两个代数运算的代数体系——环和域。首先介绍环与域的基本概念，并进一步讨论有关环的一些基本性质，最后讨论整环上的因子分解问题。

§1　环的定义

定义1　设$\{R;\ +,\ \cdot\}$是一个有两个代数运算的代数体系，如果满足下述条件：

（1）$\{R;\ +\}$是交换群；

（2）$\{R;\ \cdot\}$是半群；

（3）乘法"·"对加法"+"满足分配律，即

左分配律：$a(b+c)=ab+ac$，右分配律：$(a+b)c=ac+bc$ $(\forall a,b,c\in R)$则称$\{R;\ +,\cdot\}$是一个环，也简称R是一个环。

由于环对加法是交换群，所以交换群所具有的性质，任一环R必都具备。比如，环R中对加法来说有零元0，使

$$0+a=a+0=a,\ \forall a\in R$$

对环R中任意元素a，都有负元$-a$，使

$$a+(-a)=(-a)+a=0$$

而且，在环中还有

$$n(a+b)=na+nb$$

$$(n+m)a=na+ma$$

$$(nm)a=n(ma),\ n,\ m\text{是任意整数}$$

其次，因为$\{R;\ \cdot\}$是半群，所以关于半群的一切结论，

环 R 作为乘法半群来说，自然成立。

再次，环 R 还具有下述性质：

（1） $0a=a0=0$， $\forall a\in R$

（2） $(-a)b=a(-b)=-(ab)$， $\forall a,b\in R$

（3） $(-a)(-b)=ab$， $\forall a,\ b\in R$

事实上，由于 $0+0=0$，所以

$$a0=a(0+0)=a0+a0$$

从而有$a0=0$。同理有$0a=0$。即（1）成立。

又因

$$ab+a(-b)=a(b+(-b))=a0=0$$

所以，$a(-b)=-ab$，同理有 $(-a)b=-ab$。即（2）成立。

（3）的证明作为练习。

在环中广义分配律成立。

$$\begin{aligned}&(a_1+a_2+\cdots+a_m)(b_1+b_2+\cdots+b_n)\\&=a_1b_1+a_1b_2+\cdots+a_1b_n+a_2b_1+a_2b_2+\cdots+a_2b_n+\cdots\\&\quad+a_mb_1+a_mb_2+\cdots+a_mb_n\end{aligned}$$

应用数学归纳法，上式即可得证。

对环 R 来说，半群 $\{R;\ \cdot\}$ 有恒等元时，由本书第一章§6可知 R 的恒等元只能有一个。这时我们用1表示环 R 的恒等元，并称环 R 的恒等元为**单位元**。有单位元的环也叫做**有1的环**。

设 R 是有1的环，如果对环 R 中的元 a 来说，在 R 中存在元a'，使

$$aa'=a'a=1$$

则称a'为 a 的**逆元**，这时称 a 为 R 中的**可逆元**或**单位**。容易看出，若 a 是 R 中的可逆元，则 a 的逆元只能有一个，用 a^{-1}表示 a 的逆元。

显然，有1的环 R 中的所有可逆元（单位），关于 R 的乘法是一个群。

当环 R 的乘法满足交换律，即

$$ab=ba,\quad \forall a,\ b\in R$$

时，则称R为交换环。

例 1　整数集Z关于通常的加法和乘法，即代数体系$\{Z;+,\cdot\}$是交换环，而且是有1的交换环。Z的单位元是1，而且，Z的可逆元（单位）只有±1。

例 2　$\{Q;+,\cdot\}$和$\{R;+,\cdot\}$也都是有1的交换环，而且Q和R中的每个非0元都是可逆元。

例 3　实数域R上的全体n阶方阵$M_n(R)$关于矩阵加法和乘法是环，称它为R上的n阶全阵环。

$M_n(R)$的零元为零阵，单位阵是$M_n(R)$的单位元，可逆元是n阶可逆阵（非奇异阵）。因此，$M_n(R)$中所有可逆元所构成的乘群是n阶一般线性群$GL_n(R)$（参阅第二章§1例3）。而且，当$n\geqslant2$时，$M_n(R)$不是交换环。

例 4　$\{Z_n;+,\cdot\}$是交换环。

事实上，由第二章§1例4知$\{Z_n;+\}$是加群，由第一章§6知$\{Z_n;\cdot\}$是半群，而且容易验证，剩余类的乘法对加法满足分配律。

事实上，$\forall \overline{a},\ \overline{b},\ \overline{c}\in Z_n$，

$$\overline{a}(\overline{b}+\overline{c})=\overline{a}(\overline{b+c})=\overline{a(b+c)}=\overline{ab+ac}$$
$$=\overline{ab}+\overline{ac}=\overline{a}\,\overline{b}+\overline{a}\,\overline{c}$$

因为Z_n的乘法满足交换律，所以由上式有

$$(\overline{b}+\overline{c})\overline{a}=\overline{a}(\overline{b}+\overline{c})=\overline{a}\,\overline{b}+\overline{a}\,\overline{c}$$
$$=\overline{b}\,\overline{a}+\overline{c}\,\overline{a}$$

综上所述，可知$\{Z_n;+,\cdot\}$是交换环，称它为**整数环Z的以n为模的剩余类环，或简称为以n为模的剩余类环，或模n的剩余类环。**

显然，Z_n中的元$\overline{1}$是Z_n的单位元。进一步可以证明：**Z_n中的元$\overline{a}$是可逆元。**$\Longleftrightarrow(n,a)=1$。

事实上，若$(n,a)=1$，则由整数的性质知，存在整数b和c，使

$$nb + ac = 1$$

由此有

$$\overline{nb + ac} = \overline{1}, \quad \overline{nb} + \overline{ac} = \overline{1}$$

而 $$\overline{nb} + \overline{ac} = \overline{n}\,\overline{b} + \overline{a}\,\overline{c} = \overline{0} + \overline{a}\,\overline{c} = \overline{a}\,\overline{c}$$

所以有$\overline{a}\,\overline{c} = \overline{1}$，而$\overline{c} \in Z_n$， 即 $\overline{c}$是$\overline{a}$的逆元。所以，当 $(n, a) = 1$ 时，$\overline{a}$是 Z_n 的可逆元。

充分性的证明作为练习。

例 5 $F[x] = \{f(x) \mid f(x)$ 为数域F上的多项式$\}$关于多项式的加法和乘法是有 1 的交换环。

当环R只有一个元时，则由环的定义知，此元必为零元，这样的环叫做零环。

因为，在环R中零元 0 有性质

$$0 + 0 = 0, \quad 0 \cdot 0 = 0$$

所以，零环R中的唯一元 0，既是加群的恒等元又是R的单位元。但是，对于任一非零环R（即R中至少含有一个非零元）来说，如果R有单位元 1，则$1 \neq 0$。今后，凡是提到环R有单位元时，总是指环R不是零环，即单位元$1 \neq 0$。

习　　题

1　对环R中任二元素a、b，证明：

$(-a)(-b) = ab$

2　证明：有 1 的环中所有可逆元关于乘法构成群。

3　在环中证明广义分配律成立。

4　设R为有 1 的非零环，证明：$1 \neq 0$。

5　举出没有单位元的环的例子。

6　设R_1和R_2都是环，$R = \{(x_1, x_2) \mid x_1 \in R_1, x_2 \in R_2\}$，$\forall (x_1, x_2)$，$(y_1, y_2) \in R$，规定

$$(x_1, x_2) = (y_1, y_2) \Longleftrightarrow x_1 = y_1, \ x_2 = y_2$$

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2)$$

证明：

（1）$\{R; +, \cdot\}$ 是环；

（2）R是交换环$\Longleftrightarrow R_1$和R_2都是交换环；

（3）R_1和R_2有单位元e_1和e_2时，则$e=(e_1, e_2)$是R的单位元。

这时，$a=(a_1, a_2)$是R的可逆元（单位）$\Longleftrightarrow a_1$和a_2分别是R_1和R_2的可逆元。

7　设R为定义在$[0,1]$上所有实函数的集合。证明：R关于函数的加法和乘法是环。

8　设R为环，证明：若R关于乘法有且只有一个左恒等元e，则R是有1的环，单位元就是e。

9　若R是有1的环，如果a在R中有且只有一个左逆元a'，则a是R的可逆元，而且$a'=a^{-1}$。

10　如果对环R的元a存在正整数n，使$a^n=0$，则称a为R的幂零元。

若R是有1环的，a是R的幂零元，证明：$1-a$是R的可逆元，并求其逆元。

§2　整环、除环和域

设R为环，0为R的零元。如果对于R中的元a来说，在R中存在非零元b，使

$$ab=0\quad（或\ ba=0）$$

时，则称a为环R的左（右）零因子。

当元a在R中既是左零因子同时又是右零因子时，则称a为R的零因子。

显然，R的零元是零因子，环R中不是零元的左（右）零因子叫做R的真左（右）零因子。当然，对交换环R来说，零因子没有左、右之分。我们约定，当环R不含左、右真零因子时，称R为没有真零因子的环。显然，环R没有真零因子$\Longleftrightarrow$ $\forall a, b\in R$，若$ab=0$，则$a=0$或$b=0$。

定义1　有1的交换环R如果没有真零因子，则称环R为整环。

例 1 复数域C上的2阶全阵环 $M_2(C)$ 中的元素：$A=\begin{pmatrix}1&0\\1&0\end{pmatrix}$ 和 $B=\begin{pmatrix}0&0\\1&1\end{pmatrix}$ 分别是左（真）零因子和右（真）零因子。因为

$$AB=\begin{pmatrix}1&0\\1&0\end{pmatrix}\begin{pmatrix}0&0\\1&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

而 $A\neq 0$，$B\neq 0$。

例 2 令R为定义在〔0,1〕上所有实函数所构成的环(见§1习题7)，则R中的元

$$p(x)=\begin{cases}0 & \text{当}\quad 0\leqslant x\leqslant\frac{1}{2}\\ 1 & \text{当}\quad \frac{1}{2}<x\leqslant 1\end{cases}$$

$$q(x)=\begin{cases}1 & \text{当}\quad 0\leqslant x\leqslant\frac{1}{2}\\ 0 & \text{当}\quad \frac{1}{2}<x\leqslant 1\end{cases}$$

显然，$p(x)$和$q(x)$都不是零函数$f_0(x)$（即R的零元），但是，$p(x)q(x)\in R$，而$p(x)q(x)=f_0(x)$，所以$p(x)$和$q(x)$都是R的真零因子（因为R是交换环）。

例 3 整数环Z是整环。

例 4 实数域R上的多项式环$R[x]$是整环。

这是因为，$R[x]$是有1的交换环，而且当

$$f(x)=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0\neq 0\text{时，}a_m\neq 0$$

$$g(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0\neq 0\text{时，}b_n\neq 0$$

则

$$f(x)g(x)=a_mb_nx^{n+m}+\cdots+a_0b_0\neq 0\quad(\text{因}a_mb_n\neq 0)$$

所以，$R[x]$是整环。

定义 2 **设R为有单位元的环，$\dot{R}$表示R中所有非零元所构成的集合，如果$\{\dot{R};\ \cdot\}$是一个群，则称环R为除环或体，交换除环（体）叫做域。**

由上述定义可以看出：（1）除环是没有真零因子的环；

（2）环R是除环$\Longleftrightarrow R$中有1而且R中任意非零元都是可逆元；（3）环$\{R;\ +,\ \cdot\}$是域$\Longleftrightarrow\{R;\ +\}$和$\{\dot{R};\ \cdot\}$都是交换群。

例5　由于整数环Z中，只有± 1是可逆元，所以Z是整环但不是域。

例6　$\{Q;\ +,\ \cdot\}$，$\{R;\ +,\ \cdot\}$，$\{C;\ +,\ \cdot\}$都是域。

例7　整数环Z的以2为模所得到的剩余类环$Z_2=\{\overline{0},\ \overline{1}\}$，是域。

事实上，Z_2是有单位元的交换环，非0元只有$\overline{1}$，而$\overline{1}$是Z_2的可逆元，所以Z_2是域。

例8　当p为质数时，$\{Z_p;\ +,\ \cdot\}$是域。

事实上，Z_p是有单位元的交换环，而当p为质数时，若$\overline{a}\neq\overline{0}$，则有$p\nmid a$，从而$(p,a)=1$。于是由上节例4知$\overline{a}$为$Z_p$的可逆元。因此，$Z_p$为域。

例9　考虑复数域C上的二阶全阵环$M_2(C)$，由本节例1知$M_2(C)$既不是整环，也不是交换环，当然更不是除环。下面考虑$M_2(C)$的子集

$$K=\left\{\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}\middle|\ \alpha,\ \beta\in C\right\}$$

可以验证，

（1）关于矩阵的加法和乘法K组成一代数体系；

（2）$\{K;\ +,\ \cdot\}$是环；

（3）环K是除环但不是域。

（1）与（2）作为习题，下面来证明（3）成立。

首先，K有单位元：$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=e$。其次，对于$K$中任意非0元

$$A=\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}=\begin{pmatrix}a+bi & c+di\\ -c+di & a-bi\end{pmatrix}$$

（其中a，b，c，d是不全为0的实数）。由于

$$|A| = \begin{vmatrix} a+bi & c+di \\ -c+di & a-bi \end{vmatrix} = a^2+b^2+c^2+d^2 \neq 0$$

所以A有逆阵

$$A^{-1} = \begin{pmatrix} \frac{a-bi}{|A|} & \frac{-(c+di)}{|A|} \\ \frac{c-di}{|A|} & \frac{a+bi}{|A|} \end{pmatrix}$$

显然 $A^{-1} \in K$，而 $AA^{-1} = A^{-1}A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$，所以$K$中任意非0元素都是可逆元．总此说明$K$是除环。

最后指出K不是域。事实上，只要指出在K中至少有两个元素A，B不可换：$AB \neq BA$即可。

我们看

$$i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

通过实际计算有

$$ij = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad ji = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

所以K不是域．除环K叫做哈密尔顿（Hamilton）四元数除环，或$\mathbf{R}$上的四元数除环，简称为四元数除环．若令$\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = k$时，则有

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

而且对K中任意元A有

$$A = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$+ c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = a+bi+cj+dk$$

其中 a 是$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$的简写，因而四元数除环$K$中的元也叫四元数。

习　　题

1　证明：可逆元不是零因子.

2　设R为整环，$a(\neq 0)\in R$.若 $a^2=a$，则 $a=1$。这个结论对任意环是否一定成立？

3　找出 $\boldsymbol{R}[x]$中的可逆元，由此指出 $\boldsymbol{R}[x]$不是域。

4　证明：有 1 的交换环R是整环必要而且只要$\{\dot{R};\ \cdot\}$ 是$\{R;\ \cdot\}$的子半群。

5　证明：环 R 没有真左（右）零因子$\Longleftrightarrow$左（右）消去律成立：若$ax=ay$，且$a\neq 0$，则$x=y$（若 $xa=ya$，且$a\neq 0$，则$x=y$）.

6　环R的元素个数 $n(>1)$有限，如果R没有真零因子，则 R 是除环。

7　S是环R中一切非零因子的集合，证明：$\{S;\ \cdot\}$是半群。

8　$\{R;\ +,\ \cdot\}$是除环。证明：加群$\{R;\ +\}$与乘群 $\{\dot{R};\ \cdot\}$不能同构。

9　环$R\neq\{0\}$是除环必要而且只要$\forall a(\neq 0)$，$b\in R$，方程

$$ax=b\ （或\ ya=b）$$

在R中有解。

10　设R是有 1 的含有限个元的交换环，证明：R 的元不是可逆元（单位）就是零因子。由此证明，含有限个元的整环是域。

§3　子　　环

群论中子群对群的研究起着很重要的作用，在环的理论中子环也将对环的研究起着重要作用。

定义 1　设S为环$\{R;\ +,\cdot\}$的任一非空子集，如果对R的两个运算"$+$"和"$\cdot$"，子集S也构成一个环，则称S为环R的子环，称R为S的扩环。特别地，当R的子环S是除环（或域）时，则称S为R的子体（子域）.

例 1　全体偶数集Z_0是整数环Z的子环。

例 2　有理数域Q和实数域R是复数域C的子域。

例 3　实数域R上的多项式环$R[x]$中所有常数的集合，即R本身，是$R[x]$的子域。

显然，环R本身与$\{0\}$都是R的子环，称它们为平凡（当然）子环。

当环R是交换环时，显然R的任一子环也必为交换环。

我们在讨论群时，曾经看到群G的子群H必有恒等元而且与G的恒等元相同。但是，对于任意环R来说，不一定有单位元，所以扩环与子环就单位元来说没有必然的联系。

例 4　整数环Z有单位元，但其子环—偶数环没有单位元。

例 5　$Z_6=\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}\}$是有 1 的交换环。容易验证：

$$S_1=\{\overline{0},\ \overline{3}\}\text{和}S_2=\{\overline{0},\ \overline{2},\ \overline{4}\}$$

都是Z_6的子环。而且$\dot{S}_1=\{\overline{3}\}$和$\dot{S}_2=\{\overline{2},\ \overline{4}\}$都是乘群，所以$S_1$和$S_2$都是域。

因为，$\overline{3}\cdot\overline{3}=\overline{3}$所以上式说明，$Z_6$的乘法是$\dot{S}_1$的乘法，而且$\overline{3}$是$\dot{S}_1$的乘法恒等元（从而是$S_1$的单位元），所以$\dot{S}_1$是交换乘群，由此推得$S_1$是域。

对于$\dot{S}_2=\{\overline{2},\ \overline{4}\}$来说，因为$\overline{2}\cdot\overline{2}=\overline{4}$，$\overline{2}\cdot\overline{4}=\overline{2}$，$\overline{4}\cdot\overline{4}=\overline{4}$。所以，$Z_6$的乘法是$\dot{S}_2$的乘法，而且$\overline{4}$是$\dot{S}_2$的恒等元（从而是$S_2$的单位元），$\overline{2}$的逆元是$\overline{2}$，所以$\dot{S}_2$是交换乘群。因此，$S_2$也是域。此例说明：

（1）Z_6及其子环S_1和S_2都有单位元，但它们的单位元并不相同；

（2）Z_6有真零因子：$\overline{2}\neq 0$，$\overline{3}\neq\overline{0}$而$\overline{2}\cdot\overline{3}=\overline{0}$，但$S_1$和$S_2$都没有真零因子。

例 6　令$R=\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\middle|\ a,\ b\in C\right\}$，则$R$是$M_2(C)$的子环，$S=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\middle|\ a\in C\right\}$是$R$的子环，也是$M_2(C)$的子环。通过检验可知，

（1）$\begin{pmatrix}1&0\\0&1\end{pmatrix}$是$M_2(C)$的单位元，$\begin{pmatrix}1&0\\0&0\end{pmatrix}$是$S$的单位元；

（2）R没有单位元。

事实上，若$\begin{pmatrix}x&0\\y&0\end{pmatrix}$是$R$的单位元，则由单位元定义，必须

$$\begin{pmatrix}x&0\\y&0\end{pmatrix}\begin{pmatrix}a&0\\b&0\end{pmatrix}=\begin{pmatrix}a&0\\b&0\end{pmatrix}\begin{pmatrix}x&0\\y&0\end{pmatrix}=\begin{pmatrix}a&0\\b&0\end{pmatrix},\quad\forall\begin{pmatrix}a&0\\b&0\end{pmatrix}\in R$$

而
$$\begin{pmatrix}x&0\\y&0\end{pmatrix}\begin{pmatrix}a&0\\b&0\end{pmatrix}=\begin{pmatrix}ax&0\\ay&0\end{pmatrix}$$

所以，当$\begin{pmatrix}x&0\\y&0\end{pmatrix}$是$R$的单位元时，必须

$$\begin{pmatrix}ax&0\\ay&0\end{pmatrix}=\begin{pmatrix}a&0\\b&0\end{pmatrix}$$

故有 $ax=a$，$ay=b$。

因为$\begin{pmatrix}a&0\\b&0\end{pmatrix}$为$R$中任意元，故$a$，$b$可取复数域$C$中任意数，而$\begin{pmatrix}x&0\\y&0\end{pmatrix}$作为环$R$的单位元来说，必须是$R$中唯一确定的元。但是，对于$C$中任意二数$a$，$b$来说，使$ay=b$成立的复数$y$将随$a$与$b$的选取而变化。所以环$R$没有单位元。

由此例可以看出，扩环R没有单位元，但其子环S有单位元，而S作为$M_2(C)$的子环来说，二者的单位元也不相同。

当然，在环R及其子环S同时都有单位元时，有可能二者的单位元相同。这样的例子是很多的。例如，数域F作为$F[x]$的子环，二者的单位元相同；有理数域Q、实数域R、复数域C的单位元也都相同。

但是，对除环和域来说，如果除环（域）K是除环（域）F的子体（域）时，因为K作为乘群是F的子群，所以K与F的恒等元相同，从而K与F有相同的单位元。而且，K中的非零元c在K中的逆元与c在F中的逆元也是一致的。

当S是环R的子环时，由于S作为加群来说是R的子群。所以，S的零元与R的零元是一致的，而且S中任意元c在S中的负元与c在R中的负元也是一致的。（参阅第二章§2子

群）。

由子环的定义和第二章§2子群的判别条件容易得到

定理1 关于环R的非空子集S，下列四个条件等价：

（1）S是R的子环；

（2）$0\in S$而且$\forall a, b, c\in S\Longrightarrow a+b, ab, -c\in S$；

（3）$\forall a, b\in S\Longrightarrow a+b, -a, ab\in S$；

（4）$\forall a, b\in S\Longleftrightarrow a-b, ab\in S$.

定理2 关于除环（域）F的非空子集$K\neq\{0\}$，下列四个条件等价.

（1）K是F的子体（域）；

（2）$0\in K$, $e\in K$而且，$\forall a,b,c,d\neq 0\in K\Longrightarrow a+b, ab, -c, d^{-1}\in K$；

（3）$\forall a, b, c\neq 0\in K\Longrightarrow a-b, ab, c^{-1}\in K$；

（4）$\forall a, b\in K\Longrightarrow a-b\in K, ab^{-1}\in K\ (b\neq 0)$。

上述两个定理的证明作为练习。

设R为环，

$$C=\{c\in R|\ cx=xc,\ \forall x\in R\}$$

即C是R中所有与R的每一元相乘都可交换的元构成的，C叫做R的中心。则R的中心C是R的子环。

因为$0\in C$，所以$C\neq\phi$。而且，$\forall c_1, c_2\in C$, $c_1x=xc_1$, $c_2x=xc_2$, $\forall x\in R$。而

$$(c_1-c_2)x=c_1x-c_2x=xc_1-xc_2=x(c_1-c_2)$$

$$(c_1c_2)x=c_1(c_2x)=c_1(xc_2)=(c_1x)c_2=(xc_1)c_2$$
$$=x(c_1c_2)$$

所以，c_1-c_2, $c_1c_2\in C$。由定理1之（4）知，C是R的子环。

例7 复数域C上的二阶全阵环$M_2(C)$的子集

$$K=\left\{\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}\middle|\alpha,\ \beta\in C\right\}$$是$M_2(C)$的子体，

$$C=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\middle| a,\quad b\in \mathbf{R}\right\}$$是 $M_2(C)$ 的子域；

$$D=\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\middle| a\in \mathbf{R}\right\}$$是 $M_2(C)$ 的子域。

事实上，K，C，D 显然非空，其次

$$\forall\begin{pmatrix} \alpha_1 & \beta_1 \\ -\overline{\beta_1} & \overline{\alpha_1} \end{pmatrix},\ \begin{pmatrix} \alpha_2 & \beta_2 \\ -\overline{\beta_2} & \overline{\alpha_2} \end{pmatrix}\in K,$$

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ -\overline{\beta_1} & \overline{\alpha_1} \end{pmatrix}-\begin{pmatrix} \alpha_2 & \beta_2 \\ -\overline{\beta_2} & \overline{\alpha_2} \end{pmatrix}=\begin{pmatrix} \alpha_1-\alpha_2 & \beta_1-\beta_2 \\ -\overline{\beta_1}+\overline{\beta_2} & \overline{\alpha_1}-\overline{\alpha_2} \end{pmatrix}$$

$$=\begin{pmatrix} \alpha_1-\alpha_2 & \beta_1-\beta_2 \\ -\overline{(\beta_1-\beta_2)} & \overline{\alpha_1-\alpha_2} \end{pmatrix}\in K$$

$$\forall\begin{pmatrix} \alpha_2 & \beta_2 \\ -\overline{\beta_2} & \overline{\alpha_2} \end{pmatrix}\neq 0\ ,\ \begin{vmatrix} \alpha_2 & \beta_2 \\ -\overline{\beta_2} & \overline{\alpha_2} \end{vmatrix}=\alpha_2\overline{\alpha_2}+\beta_2\overline{\beta_2}$$

$$=|\alpha_2|^2+|\beta_2|^2\neq 0$$

$$\begin{pmatrix} \alpha_2 & \beta_2 \\ -\overline{\beta_2} & \overline{\alpha_2} \end{pmatrix}^{-1}=\frac{1}{\begin{vmatrix} \alpha_2 & \beta_2 \\ -\overline{\beta_2} & \overline{\alpha_2} \end{vmatrix}}\begin{pmatrix} \overline{\alpha_2} & -\beta_2 \\ \overline{\beta_2} & \alpha_2 \end{pmatrix}\in K$$

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ -\overline{\beta_1} & \overline{\alpha_1} \end{pmatrix}\begin{pmatrix} \alpha_2 & \beta_2 \\ -\overline{\beta_2} & \overline{\alpha_2} \end{pmatrix}=\begin{pmatrix} \alpha_1\alpha_2-\beta_1\overline{\beta_2} & \alpha_1\beta_2+\beta_1\overline{\alpha_2} \\ -\overline{\beta_1}\alpha_2-\overline{\alpha_1}\,\overline{\beta_2} & -\overline{\beta_1}\beta_2+\overline{\alpha_1}\,\overline{\alpha_2} \end{pmatrix}$$

$$=\begin{pmatrix} \alpha_1\alpha_2-\beta_1\overline{\beta_2} & \alpha_1\beta_2+\beta_1\overline{\alpha_2} \\ -\overline{(\alpha_1\beta_2+\beta_1\overline{\alpha_2})} & \overline{\alpha_1\alpha_2-\beta_1\overline{\beta_2}} \end{pmatrix}\in K$$

所以，由定理 2 之（3），K是 $M_2(C)$的子体。

由上面的验证，显然可以看出C 也是 $M_2(C)$ 的 子 体。但是，因为

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

$$\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

所以，C 是子域。

对于 D 来说，$\forall \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix}$，$\begin{pmatrix} a_2 & 0 \\ 0 & a_2 \end{pmatrix} \in D$

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} - \begin{pmatrix} a_2 & 0 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & 0 \\ 0 & a_1 - a_2 \end{pmatrix} \in D$$

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ 0 & a_2 \end{pmatrix}^{-1} = \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} a_2^{-1} & 0 \\ 0 & a_2^{-1} \end{pmatrix} = \begin{pmatrix} a_1 a_2^{-1} & 0 \\ 0 & a_1 a_2^{-1} \end{pmatrix} \in D$$

$$\begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_2 & 0 \\ 0 & a_2 \end{pmatrix}\begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & 0 \\ 0 & a_1 a_2 \end{pmatrix}$$

所以，D 是 $M_2(C)$ 的子域。

例 8 设 $\{S_\lambda\}_{\lambda \in \Lambda}$ 是环 R 的若干个子环，则 $\bigcap\limits_{\lambda \in \Lambda} S_\lambda$ 是 R 的子环；除环 F 的一个子体族：$\{K_\mu\}_{\mu \in M}$ 的交 $\bigcap\limits_{\mu \in M} K_\mu$ 是 F 的子体。

证明 因为，$0 \in S_\lambda$，$\forall \lambda \in \Lambda$，所以 $\bigcap\limits_{\lambda \in \Lambda} S_\lambda$ 非空。

$\forall a, b \in \bigcap\limits_{\lambda \in \Lambda} S_\lambda$，则 $a, b \in S_\lambda$，$\forall \lambda \in \Lambda$。

因为 S_λ 是 R 的子环，所以有 $a-b \in S_\lambda$，$ab \in S_\lambda$，$\forall \lambda \in \Lambda$。从而 $a-b \in \bigcap\limits_{\lambda \in \Lambda} S_\lambda$，$ab \in \bigcap\limits_{\lambda \in \Lambda} S_\lambda$，

故由定理 1 之（4），$\bigcap\limits_{\lambda \in \Lambda} S_\lambda$ 是 R 的子环。

根据交的性质应用定理 2，即可证得 $\bigcap\limits_{\mu \in M} K_\mu$ 是 F 的子体。

习　　题

1　验证复数域 $\mathbf{C}$ 的子集：

$S = \{a + bi \mid a, b \in \mathbf{Z}\}$ 是 $\mathbf{C}$ 的子环；

$K = \{a + bi \mid a, b \in \mathbf{Q}\}$ 是 $\mathbf{C}$ 的子环；

2　$\mathbf{R}[x]$ 的子集 $S = \{f(x^2) \mid f(x) \in \mathbf{R}[x]\}$ 是 $\mathbf{R}[x]$ 的子环。

3　设 $\mathbf{R}$ 是有单位元 1（$\neq 0$）的交换环，S 是含 1 的 R 的子环，a_1，a_2，…，$a_n \in R$。令

$S[a_1, a_2, \cdots, a_n] = \{\Sigma C_{k_1 k_2 \cdots k_n} a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$（有限和）$C_{k_1 k_2 \cdots k_n} \in S$，$k_1 \geqslant 0$，$k_2 \geqslant 0$，$\cdots k_n \geqslant 0\}$

其中 $a_i \neq 0$ 时，$a_i^{k_i} = \begin{cases} a_i a_i \cdots a_i \ (k_i \text{个}) & k_i > 0 \text{时} \\ 1 & k_i = 0 \text{时}, \end{cases}$ $a = 0$ 时，$a_i^{k_i} = 0$。

证明，$S[a_1, a_2, \cdots, a_n]$ 是 R 的子环而且是 R 的含 S 和 a_1，a_2，$\cdots a_n$ 的

最小子环，即若$\overline{S}$是R的子环且$\overline{S}\supseteq S;a_1, a_2, \cdots, a_n\in\overline{S}$，则必有$\overline{S}\supseteq S[a_1, a_2, \cdots, a_n]$，

4　指出习题1中$\mathbf{C}$的子环$S=\mathbf{Z}[i]$，$\mathbf{C}$的子域$K=\mathbf{Q}[i]$。

5　对习题3的记号$S[a_1, a_2, \cdots, a_n]$证明：

$S[a_1, a_2]=S[a_1][a_2]$

6　求二阶全阵环$M_2(\mathbf{C})$的中心。

7　S为环R的非空子集，令

$C(S)=\{r\in R\,|\,rx=xr,\ \forall x\in S\}$

证明$C(S)$是R的子环。

8　R是环，如果$a\in R$，$a^2=a$时，则称a为R的幂等元。

（1）如果在环R中没有非零幂零元，则R的任意幂等元a与R的每一元素x可交换

$ax=xa,\ \forall x\in R,\ a^2=a$

（2）交换环R中所有幂零元的集合是R的子环。

9　令$S_p=\{\frac{a}{b}\in\mathbf{Q}\,|\,a,\ b\in\mathbf{Z},\ p\nmid b\}$，（$p$是素数）。证明$S_p$是有理数域$\mathbf{Q}$的子环。

§4　矩　阵　环

读者在“高等代数”中，对矩阵和行列式已经非常熟悉，而且对它们的重要作用也深有体会.本节将把它们进行推广，作为环的例子进行讨论。把组成数域F上的矩阵的元素推广为任意环中的元素，并进一步给出交换环上的矩阵的行列式的概念和一些在高等代数中所得到的结果。以备后面章节的应用。

令R是环，m、n是任意正整数。

定义1　由R中$m\times n$个元a_{ij}（$i=1, 2, \cdots, m$；$j=1, 2, \cdots, n$）所排成的如下形式的表

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \tag{1}$$

叫做R上的$m\times n$（或m行n列）矩阵，a_{ij}叫做矩阵的元。当$m=n$时，$n\times n$矩阵叫做n阶方阵。

以后为了书写方便，（1）形的矩阵常简写作

$$(a_{ij}),\ i=1,\ 2,\ \cdots,\ m;\ j=1,\ 2,\ \cdots,\ n$$

并把环R上的矩阵(a_{ij})用大写拉丁字母A，B，…表示。

与数域F上的矩阵相仿，规定矩阵相等、加法、乘法和纯量乘法如下：

$A=(a_{ij})$和$B=(b_{ij})$都是R上$m\times n$矩阵，规定：

$$A=B\iff a_{ij}=b_{ij}$$

加法：$(a_{ij})+(b_{ij})=(a_{ij}+b_{ij})$；

乘法：$A=(a_{ij})$为R上$m\times n$矩阵，$B=(b_{jk})$为R上$n\times s$矩阵，$AB=(c_{ik})$，$c_{ik}=\sum\limits_{j=1}^{n}a_{ij}b_{jk}$，$i=1,\ 2,\ \cdots,\ m$；$k=1,\ 2,\ \cdots,\ s$；

纯量乘法：$k(a_{ij})=(ka_{ij})$。

用0表示元素都是R的零元的矩阵，叫做**零阵**。

若$A=(a_{ij})$，则$(-a_{ij})$叫做A的**负阵**，记作$-A$，规定$A-B=A+(-B)$。

容易看出R上所有n阶方阵的集合$M_n(R)$（今后$M_n(R)$总是用来表示R上所有n阶方阵的集合）关于矩阵加法是一个加群。

而且进一步通过验证可以知道$\{M_n(R);\ +,\ \cdot\}$是一个环。

在高等代数中验证数域F上的n阶全阵环$M_n(R)$的运算所满足的算律时，只用到了F是加群和$\dot{F}$是半群以及乘法对加法满足分配律。对于环R上的n阶方阵集合$M_n(R)$来说，它的加法与乘法的规定与$M_n(F)$的规定完全一致，而且R和$\dot{R}$分别也是加群和半群，乘法对加法也满足分配律。因此，容易想象，完全可以仿照$M_n(F)$的作法验证$M_n(R)$是环。作为练习请读者自己验证。

若R是有1的环时，n阶方阵

$$E_n=\begin{pmatrix}1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}$$

叫做R上的**单位矩阵**（E_n中未标出的元素都是0）。可以验证：$E_mA=A$，$AE_n=A$，此处A为$m\times n$矩阵。

综合上述可知，若R是有1的环，则$\{M_n(R)；+，\cdot\}$也是有1的环。这时，$M_n(R)$中所有可逆元的集合$L_n(R)$关于矩阵乘法是乘群，

令E_{ij}是i行j列元素是1，其余元素皆为0的n阶方阵。n^2个n阶方阵$E_{ij}(i,\ j=1,\ 2,\ \cdots,\ n)$叫做**矩阵单位**。

关于矩阵单位，可以验证有下面的关系式：

（1）$E_{ij}E_{kl}=\delta_{jk}E_{il}$，$\delta_{jj}=1$，$\delta_{jk}=0$，$j\neq k$时；

（2）$E_{11}+E_{22}+\cdots+E_{nn}=E_n$，$E_{ii}^2=E_{ii}$；

（3）$A=(a_{ij})=\sum\limits_{i,j=1}^{n}a_{ij}E_{ij}$，$\forall A\in M_n(R)$。

由（1）可知，每个矩阵E_{ij}都是$M_n(R)$的真零因子，因此，矩阵单位并不是$M_n(R)$的单位（即可逆元）。

在上面已经指出，当R是有1的环时，则$M_n(R)$也是有1的环，这时把$M_n(R)$中可逆元A的逆元A^{-1}叫做A的**逆阵**。

对于有1的交换环R，可引进行列式的概念。关于行列式读者在高等代数中已很熟悉，并且看到行列式在线性代数中的工具作用。

设R是有1的交换环，$A=(a_{ij})\in M_n(R)$。

定义2　A的行列式用符号$\det A$或

$$\begin{vmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdots & \cdots & \cdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{vmatrix}$$

表示。

$$\det A=\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

$$=\sum_{j_1j_2\cdots j_n}(-1)^{\tau(j_1j_2\cdots j_n)}a_{1j_1}a_{2j_2}\cdots a_{nj_n}$$

此处，$\tau(j_1j_2\cdots j_n)$表示n元排列$j_1j_2\cdots j_n$的反序数，$\sum\limits_{j_1j_2\cdots j_n}$表示对所有$n$元排列求知。

按照上述定义，可以证明：数域F上n阶方阵的行列式的有关结果，对域上的n阶方阵的行列式也成立。为节省篇幅只给出几个有关结论，而不加证明。

在$A=(a_{ij})$中划去A的第i行和第j列的元素所得到的$n-1$阶方阵的行列式M_{ij}叫做a_{ij}的余子式，$(-1)^{i+j}M_{ij}$叫做a_{ij}的代数余子式，用A_{ij}表示。我们有

（1）$\det A=a_{i1}A_{i1}+a_{i2}A_{i2}+\cdots+a_{in}A_{in}$

$\quad=a_{1j}A_{1j}+a_{2j}A_{2j}+\cdots+a_{nj}A_{nj}$,

$i,j=1,2,\cdots,n$

$a_{i1}A_{j1}+a_{i2}A_{j2}+\cdots+a_{in}A_{jn}=0\quad(i\neq j)$

$a_{1i}A_{1j}+a_{2i}A_{2j}+\cdots+a_{ni}A_{nj}=0$

（2）$\det(AB)=(\det A)(\det B)$

（3）

$$\tilde{A}=\begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \cdots & \cdots & & \cdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix},$$ 其中A_{ij}为$A=(a_{ij})$中元素a_{ij}的代数余子式。叫做A的伴随阵。

由矩阵乘法可知

$$A\tilde{A}=\tilde{A}A=\begin{pmatrix} \det A & & & \\ & \det A & & \\ & & \ddots & \\ & & & \det A \end{pmatrix}=\det AE.$$

定理 若 R 是有1的交换环，则 $A\in M_n(R)$ 有逆阵（即 A 是 $M_n(R)$ 的可逆元），必要而且只要 $\det A$ 是 R 的可逆元。

证明 若 A 有逆阵 A^{-1}，则 $AA^{-1}=E_n$，而

$$\det(AA^{-1})=(\det A)(\det A^{-1})=\det E_n=1$$

所以 $\det A$ 是 R 的可逆元。反之，若 $\det A$ 是 R 的可逆元，则在 R 中有 $(\det A)^{-1}$。这时，

$$A[(\det A)^{-1}\widetilde{A}]=(\det A)^{-1}(A\widetilde{A})$$
$$=(\det A)^{-1}\det AE_n=E_n$$
$$[(\det A)^{-1}\widetilde{A}]A=(\det A)^{-1}(\widetilde{A}A)=(\det A)^{-1}\det AE_n$$
$$=E_n$$

所以，$(\det A)^{-1}\widetilde{A}$ 是 A 的逆阵。证完。

由于域 F 中每个非零元都是可逆元，所以有

推论 1 若 F 是域，则 $A\in M_n(F)$ 有逆阵必要而且只要 $\det A\neq 0$。

推论 2 R 是有1的交换环，$\forall A,\ B\in M_n(R)$，如果 $AB=E_n$，则 $B=A^{-1}$，从而有 $BA=E_n$。

证明 若 $AB=E_n$，则由 $\det(AB)=(\det A)(\det B)=1$，推得 $\det A$ 是 R 的可逆元。于是由定理，A 有逆阵 A^{-1}，用 A^{-1} 左乘 $AB=E_n$ 两边，得到

$$A^{-1}(AB)=A^{-1}E_n=A^{-1}$$

而

$$A^{-1}(AB)=(A^{-1}A)B=E_nB=B$$

所以，$B=A^{-1}$。$BA=A^{-1}A=E_n$。证完。

例 令 $R=Z_2=\{\overline{0},\overline{1}\}$。则 $M_2(R)=\left\{\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\middle|\ a_{ij}\in R\right\}$ 是一个有1，有真零因子的非交换环。

事实上，$\begin{pmatrix}\overline{1} & \overline{0}\\ \overline{0} & \overline{1}\end{pmatrix}$ 是 $M_2(R)$ 的单位元；而

$$\begin{pmatrix}\overline{0} & \overline{0}\\ \overline{1} & \overline{1}\end{pmatrix}\begin{pmatrix}\overline{0} & \overline{1}\\ \overline{0} & \overline{1}\end{pmatrix}=\begin{pmatrix}\overline{0} & \overline{0}\\ \overline{0} & \overline{0}\end{pmatrix}=0$$

$$\begin{pmatrix}\bar{0} & \bar{1}\\ \bar{0} & \bar{1}\end{pmatrix}\begin{pmatrix}\bar{0} & \bar{0}\\ \bar{1} & \bar{1}\end{pmatrix}=\begin{pmatrix}\bar{1} & \bar{1}\\ \bar{1} & \bar{1}\end{pmatrix}\neq 0$$

习　　题

1　设R不是零乘环（即存在a，$b\in R$，$ab\neq 0$），证明，$M_n(R)$在$n>1$时不是交换环。

2　判断$M_3(\mathbf{Z})$中的矩阵

$$A=\begin{pmatrix}1 & 5 & 0\\ 0 & 1 & -1\\ -3 & -5 & -9\end{pmatrix},\quad B=\begin{pmatrix}1 & 2 & 3\\ 0 & 2 & 3\\ 0 & 0 & 1\end{pmatrix}$$

有没有逆阵（在$M_3(\mathbf{Z})$中），如果有试找出之。

3　试给出$M_n(R)$（R为有1的交换环）中的矩阵

$$A=\begin{pmatrix}a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n\end{pmatrix}$$

在$M_n(R)$中有逆阵的条件。

4　若R是域，证明，$A\in M_n(F)$是零因子，必要而且只要A在$M_n(F)$中没有逆阵。这个结论对任意有1的交换环R是否也成立。

5　若R是有1的环，$p\in R$。

（1）$E_n+pE_{ij}(i\neq j)$是$M_n(R)$中的可逆元（在$M_n(R)$中有逆阵）；

（2）$E_n+(p-1)E_{ii}$在何时是$M_n(R)$的可逆元；

（3）试用$E_n+pE_{ij,i\neq j}$和$E_n+(p-1)E_{ii}$乘A，探讨一下所得到的结果与A的关系。

6　证明本节所列出的关于行列式的结果。

7　举出一个含有限个元，但没有1的非交换环的例子。

§5　理想与商环（差环）

在第二章讨论群的理论时，看到正规子群有着特殊的作用。相当于群的正规子群，在环的子环中有一类特殊的子环

——理想，通过它可以去掌握环的构造。

定义1 环R的子环N如果满足条件：

（1）$\forall r\in R,\ a\in N,\ \Longrightarrow ra\in N$，则称$N$为$R$的左理想；

（2）$\forall r\in R,\ a\in N,\ \Longrightarrow ar\in N$，则称$N$为$R$的右理想。

特别地，当N既是R的左理想又是R右理想时，则N叫做R的双边理想，简称为R的理想。

显然，当R是交换环时，左理想、右理想、双边理想三者是一致的。

命题1 环R的非空子集N是R的左（右）理想，必要而且只要

（1）$\forall a,\ b\in N\Longrightarrow a-b\in R$；

（2）$\forall a\in N,\ r\in R\Longrightarrow ra(ar)\in N$。

证明 必要性是显然的。下面证明充分性。

由（1）和（2）可知N是R的子环，再由（2）即知N是R的左（右）理想。证完。

例1 环R的平凡子环$\{0\}$和R都是R的理想，称它们为环R的平凡（当然）理想。

例2 整数环Z的子集

$$N=\{m\text{ 的一切倍数}\}$$

是Z的理想。

例3 $F[x]$是数域F上的多项式环

$$N=\{f(x)\in F[x]\mid f(1)=0\}$$

是$F[x]$的理想。

解 因$F[x]$是交换环，所以只证N满足左理想的条件即可。显然，N非空。$\forall f(x),\ g(x)\in N$，则$f(1)=0,\ g(1)=0$。令$f(x)-g(x)=h(x)$，由多项式值的性质有$h(1)=f(1)-g(1)=0-0=0\Longrightarrow f(x)-g(x)\in N$。

$\forall f(x)\in N,\ r(x)\in F[x]$，令$r(x)f(x)=k(x)$，则$k(1)=$

$r(1)f(1)-r(1)\cdot 0=0 \Longrightarrow r(x)f(x)\in N$。

于是由命题1，N是$F[x]$的左理想，从而N是$F[x]$的理想。

例4　设R是有1的环，a_1，a_2，…，$a_n\in R$。令

$$N=\{x_1a_1+x_2a_2+\cdots+x_na_n \mid x_i\in R\}$$

则N是R的左理想而且是含a_1，a_2，…，a_n的R的最小左理想，意即，若L为R的左理想而且每个a_i都在L中，则$L\supseteq N$。

上述形式的左理想N叫做R的由a_1，a_2，…，a_n所生成的左理想。

解　显然，$N\neq\phi$而且$\forall x=x_1a_1+x_2a_2+\cdots+x_na_n$，$y=y_1a_1+y_2a_2+\cdots+y_na_n\in N$，$r\in R$。

$$\begin{aligned}x-y&=(x_1a_1+x_2a_2+\cdots+x_na_n)-(y_1a_1+y_2a_2+\cdots+y_na_n)\\&=(x_1-y_1)a_1+(x_2-y_2)a_2+\cdots+(x_n-y_n)a_n\end{aligned}$$

而　$x_i-y_i\in R$，所以$x-y\in N$。

$$\begin{aligned}rx&=r(x_1a_1+x_2a_2+\cdots+x_na_n)\\&=r(x_1a_1)+r(x_2a_2)+\cdots+r(x_na_n)\\&=(rx_1)a_1+(rx_2)a_2+\cdots+(rx_n)a_n\end{aligned}$$

而　$rx_i\in R$，所以，$rx\in N$。

于是由命题1知N是R的左理想。因为R有1，故有

$$a_i=0a_1+\cdots+0a_{i-1}+1\cdot a_i+0a_{i+1}+\cdots+0a_n$$

所以$a_i\in N$。

其次说明N的最小性。

若L是R的左理想，且a_1，a_2，…，$a_n\in L$。于是由左理想的定义，$\forall x_1$，x_2，…，$x_n\in R$，必有x_1a_1，x_2a_2，…，$x_na_n\in L$。进一步，因左理想是子环，故有

$$x_1a_1+x_2a_2+\cdots+x_na_n\in L$$

上述事实说明，L包含N中的所有元，即$L\supseteq N$。

例5　若F为域，则F的理想只能是$\{0\}$或F。

解　设N是F的理想，如果$N\neq\{0\}$，则在N中至少有$a\neq$

0。因为 F 为域，故有 $a^{-1}\in F$。

因 N 为 F 的理想，则取 $a^{-1}\in F$，$a\in N$，必有 $a^{-1}a=1\in N$。而对于 F 中任意元 x，$x=x\cdot 1\in N$。所以，$N=F$。由此得知，域 F 的理想只能是 $\{0\}$ 或 F。

下面对任意环 R 给出一种构造理想的方法。令 R 为环，$a\in R$，

$N=\{x_1ay_1+x_2ay_2+\cdots+x_say_s+xa+ay+na \mid x_i,\ y_i,\ x,\ y\in R,\ n$ 为任意整数$\}$

则 N 是 R 的理想。事实上，$N\neq\phi$，而且对于 N 中任意二元

$$x_1ay_1+\cdots+x_say_s+xa+ay+na \text{ 和 } x_1'ay_1'+\cdots+x_t'ay_t'+x'a+ay'+n'a$$

来说

$$(x_1ay_1+\cdots+x_say_s+xa+ay+na)-(x_1'ay_1'+\cdots+x_t'ay_t'+xa'+ay'+n'a)=x_1ay_1+\cdots+x_say_s+(-x_1')ay_1'+\cdots+(-x_t')ay_t'+(x-x')a+a(y-y')+(n-n')a\in N$$

$$\begin{aligned}&r(x_1ay_1+\cdots+x_say_s+xa+ay+na)\\&=(rx_1)ay_1+\cdots+(rx_s)ay_s+(rx)a+ray+r(na)\\&=(rx_1)ay_1+\cdots+(rx_s)ay_s+ray+[(rx)+nr]a\in N\end{aligned}$$

所以，N 是 R 的理想。

按上述方式所得到的理想 N 叫做由 a **生成的主理想**，记作：(a)。容易看出，(a) 是环 R 的含 a 的最小理想。特别地，若 R 是有 1 的环时，则

$(a)=\{x_1ay_1+\cdots+x_say_s \mid x_i,\ y_i\in R\}$

当 R 是有 1 的交换环时，则由 a 所生成的主理想 $(a)=\{ra \mid r\in R\}$。

对任意环 R 来说，可将构造主理想的方法推广，给出由环 R 的 n 个元：a_1，a_2，…，a_n，构造一个环 R 的含 a_1，a_2，…，a_n 的最小理想。令

$$N=\{s_1+s_2+\cdots+s_n \mid s_i\in(a_i),\ i=1,\ 2,\ \cdots,\ n\}$$

其中(a_i)是R的由a_i所生成的主理想．则N是R的含a_1，a_2，…，a_n的最小理想．

事实上，$N \neq \phi$，而且$\forall a$，$a' \in N$

$a = s_1 + s_2 + \cdots + s_n$，$a' = s'_1 + s'_2 + \cdots s'_n$，$s_i$，$s'_i \in (a_i)$

因为，$s_i - s'_i \in (a_i)$，$i = 1, 2, \cdots, n$；rs_i，$s_i r \in (a_i)$，$\forall r \in R$，$i = 1$，2，$\cdots, n$．所以

$a - a' = (s_1 - s'_1) + (s_2 - s'_2) + \cdots + (s_n - s'_n) \in N$

$ra = rs_1 + rs_2 + \cdots + rs_n \in N$

$ar = s_1 r + s_2 r + \cdots + s_n r \in N$

因此，N是R的理想，至于N是含$a_1, a_2, \cdots, a_n$的最小理想是显然的。

我们称N是R的由$a_1, a_2, \cdots, a_n$，所生成的理想，记作：$(a_1, a_2, \cdots, a_n)$。

例6 例2中整数环Z的理想N是主理想：$N = (m)$。

定义2 **如果整环R的理想都是主理想，则称R为主理想环。**

例7 本节例3中$F[x]$的理想$N = \{f(x) \in F[x] \mid f(1) = 0\}$是由$x-1$所生成的主理想．

解 由多项式根的性质知，$f(1) = 0 \Longleftrightarrow x - 1 \mid f(x)$，即$f(x) = q(x)(x-1)$，$q(x) \in F[x]$。

上述性质说明，N中的元必在$x-1$所生成的主理想中；另一方面，由$x-1$所生成的主理想中的元都是形如：$q(x)(x-1) = g(x)$的元，显然，$g(1) = 0$。所以$N = (x-1)$。

例8 整数环Z是主理想环．

解 首先，Z是整环，其次令N为Z的任意理想，去证N是主理想。

若$N = \{0\}$，显然N是主理想。

若$N \neq \{0\}$，则N中一定有$a \neq 0$．由N为理想，则$-a \in N$。这时，a与$-a$中必有一是正数

令c是N中最小的正数，去证$N = (c)$。对N中任一元b

来说，由带余除法有

$$b = qc + r, \quad 0 \leqslant r < c$$

因为，b, $c \in N$，所以 $r = b - qc \in N$。由$r < c$及 c 是N中的最小正数，所以 $r = 0$ 即 $b = qc$。

上述事实说明：N中的任一元皆在 (c)中，故有$N \subseteq (c)$，另一方面，由于 $c \in N$ ，则根据 (c) 是含 c 的最小理想，推得 $N = (c)$。

在群论中我们已经看到了正规子群的作用是非常重要的，面理想在环论中的作用与正规子群在群论中的作用很类似。设N是环R的理想。从群的角度看，R是加群，N是R的子群而且是R的正规子群。于是，由第二章§ 7 R对N的商集$R/N = \{x + N | x \in R\}$ 关于陪集的加法也构成一个加群。

进一步，在R/N中规定

$$(x + N)(y + N) = xy + N, \quad x, \ y \in R$$

下面来说明，上述规定是R/N的代数运算。为此需证明：若 $x + N = x' + N$, $y + N = y' + N$,则 $xy + N = x'y' + N$,即上述规定与代表的选择无关。为此只须证 $xy - x'y' \in N$ 即可，事实上，由

$$x + N = x' + N \Longrightarrow x - x' \in N; y + N = y' + N \Longrightarrow$$
$$y - y' \in N$$

所以有 n_1, $n_2 \in N$，使

$$x - x' = n_1, \quad 即\ x = x' + n_1$$
$$y - y' = n_2, \quad 即\ y = y' + n_2$$

而

$$xy = (x' + n_1)(y' + n_2) = x'y' + n_1y' + x'n_2 + n_1n_2$$

因为N为理想，所以 n_1y', $x'n_2$, n_1n_2 都在N中，所以

$$xy - x'y' = n_1y' + x'n_2 + n_1n_2 \in N$$

综上所述，可知上面所规定的是R/N的代数运算。

定理 R为环，N是R的理想。则R对N的商集R/N关于下面的加法和乘法构成环。

加法　$(n+N)+(y+N)=(x+y)+N$；

乘法　$(x+N)(y+N)=xy+N$，$x,y\in R$。

证明　由第二章§7已知$\{R/N;\ +\}$是加群．其次，

$$(x+N)[(y+N)(z+N)]=x(yz+N)=x(yz)+N$$

$$[(x+N)(y+N)](z+N)=(xy+N)(z+N)$$
$$=(xy)z+N$$

因为R的乘法满足结合律，所以

$$(x+N)[(y+N)(z+N)]=[(x+N)(y+N)](z+N)$$

即R/N的乘法满足结合律，故$\{R/N;\ \cdot\}$是半群．

因为R/N的加法和乘法是由R的加法和乘法确定的，所以仿上，根据R的乘法对加法满足分配律，容易看出R/N的乘法对R/N的加法也满足分配律。综上所述，$\{R/N;\ +,\ \cdot\}$是环。证完。

从上述证明中看出，若R有1则R/N也有1；若R是交换环则R/N也是交换环。

定理中的环R/N叫做R对N的商环或差环，也有人称它为以N为模的剩余类环。

例9　Z是整数环，n是大于0的整数，可知(n)是Z的理想．则$\mathbf{Z}/(n)=\{0+(n)=\overline{0},\ 1+(n)=\overline{1},\ \cdots,\ (n-1)+(n)=\overline{n-1}\}$。

即整数环Z对理想$N=(n)$的商环是以n为模的剩余类环$\mathbf{Z}_n$。

例10　$\mathbf{Z}[i]=\{a+bi\,|\,a,\ b\in\mathbf{Z}\}$是有1的交换环，$N=\{2(a+bi)\,|\,a,b\in\mathbf{Z}\}$是$\mathbf{Z}[i]$的理想．求出$\mathbf{Z}[i]$对$N$的商环$\mathbf{Z}[i]/N$的所有元素。

解　因为对于任意整数n，都有

$$n=2q+r,\quad 0\leqslant r<2$$

所以，对$\mathbf{Z}[i]$中任意元$a+bi$有

$$a+bi=(2a_1+a_2)+(2b_1+b_2)i=2(a_1+b_1i)+(a_2+b_2i)$$

其中，$0\leqslant a_2<2$，$0\leqslant b_2<2$。因此，$\mathbf{Z}[i]$中满足条件：

$0\leqslant a_2<2$，$0\leqslant b_2<2$的数：a_2+b_2i所在的陪集即为$\mathbf{Z}[i]/N$的所有元．而 $\mathbf{Z}[i]$ 中满足上述条件的数只有下列四个：0，1，i，$1+i$．所以，

$$\mathbf{Z}[i]/N=\{0+N,1+N,i+N,(1+i)+N\}$$

习　　题

1　验证：$N=\left\{\begin{pmatrix}a_1 & 0\\ a_2 & 0\end{pmatrix}\middle|\ a_1,\ a_2\in R\right\}$是环$R$上的二阶全阵环$M_2((R)$的左理想；$N_2=\left\{\begin{pmatrix}b_1 & b_2\\ 0 & 0\end{pmatrix}\middle|\ b_1,\ b_2\in R\right\}$是 $M_2(R)$ 的右理想，但都不是双边理想。

2　设I和J为环R的（左、右、双边）理想，则$I+J=\{u+v|u\in I,\ v\in J\}$是$R$的（左、右、双边）理想。

3　设R为整环，a，$b\mid R$．试给出$(a)=(b)$的条件。

4　设 $N=\{n(a+bi)\mid a+bi\in\mathbf{Z}[i]\}$，$n$ 为大于 1 的整数，试确定$\mathbf{Z}[i]/N$ 的元的个数．（此处承认N是$\mathbf{Z}[i]$的理想）．

5　$F[x]$是数域F上的多项式环，(x^2-1)是 $F[x]$的由x^2-1所生成的主理想，指出$F[x]/(x^2-1)$不是整环。

6　证明整数环$\mathbf{Z}$的由 4 和 9 所生成的理想$(4,\ 9)=(1)$。

7　证明数域F上的多项式环$F[x]$的理想：$(2,\ x)$是主理想。

8　证明，（1）若N是环R的左理想，则

$A=\{x\in R|\ xn=0,\ \forall n\in N\}$

是R的理想，叫做N在R中的左零化子；

（2）若N是环R的右理想，则

$B=\{y\in R|\ ny=0,\ \forall n\in N\}$

是R的理想，叫做N在R中的右零化子．

§6　环的同态与同态基本定理

相当于群与其每一商群间的关系，环R与其每一商环R/N间也有着类似的结果．本节将给出环R与其商环以及R的同态象与R的商环间的关系．在第一章介绍了有两个代数运算的代数体系的同态与同构的概念．当然这两个概念可以适用于环．

下面再重新明确一下环的同态与同构的概念。设 R 和 R' 是两个环，如果 φ 是 R 到 R' 的满射，且满足条件

（1）$\varphi(x+y)=\varphi x+\varphi y$；

（2）$\varphi(xy)=(\varphi x)(\varphi y)$，$\forall x,\ y\in R$

时，φ 叫做 R 到 R' 的满同态；如果对环 R 和 R' 存在 R 到 R' 的满同态 φ 时，则说 R 与 R' 同态，记作：$R\sim R'$，或 $R\underset{\sim}{\varphi}R'$。

当满同态 φ 又是单射时，则称 φ 为 R 到 R' 的同构映射，这时就说 R 与 R' 同构，记作：$R\cong R'$。

关于环的同态也有相当于群的同态的一些结果。设 R 是一个环，$\{R';\ \oplus,\ \odot\}$ 是有两个代数运算的代数体系，由第一章§5和第二章§3有：

命题1 若存在环 R 到 R' 的满同态 φ，则 R' 也是环。

命题2 若环 R 与环 R' 同态：$R\overset{\varphi}{\sim}R'$，则

（1）R 的零元的象 $\varphi(0)$ 是 R' 的零元；

（2）环 R 中元 a 的负元 $-a$ 的象 $\varphi(-a)$ 是 a 的象的负元，即

$$\varphi(-a)=-\varphi(a)$$

（3）若 R 是交换环则 R' 也是交换环；

（4）若 R 有 1，则 $\varphi(1)$ 是 R' 的单位元。

命题3 若环 R 与环 R' 同构，则

R 是整环（除环、域）$\Longleftrightarrow R'$ 是整环（除环、域）

上述三个命题的证明作为练习。

若 φ 是环 R 到 R' 的满同态，环 R' 中的零元在 φ 之下的完全原象 N 叫做 φ 的核，记作：$N=\mathrm{Ker}\varphi$。

命题4 环 R 到环 R' 的任一满同态 φ 的核都是 R 的理想。

证明 显然，$\mathrm{Ker}\varphi\neq\phi$，$\forall x,\ y\in\mathrm{Ker}\varphi$，则由同态核的定义，$\varphi(x)=0$，$\varphi(y)=0$，而

$$\varphi(x-y)=\varphi(x)+\varphi(-y)=\varphi(x)-\varphi(y)=0-0=0$$

$$\varphi(rx)=\varphi(r)\ \varphi(x)=\varphi(r)\cdot 0=0$$

$$\varphi(xr)=\varphi(x)\varphi(r)=0\cdot\varphi(r)=0\ ,\quad \forall r\in R$$

所以，由核的定义有$x-y$，rx，$xr\in \mathrm{Ker}\varphi$。上述说明$\mathrm{Ker}\varphi$是$R$的理想。

命题 5 若φ是环R到环R'的满同态，而$\mathrm{Ker}\varphi=\{0\}$，则$\varphi$是同构映射。

证明 只须证明φ是单射即可。

$\forall x,\ y\in R$，若$\varphi(x)=\varphi(y)$，则有$\varphi(x)-\varphi(y)=0$。因φ是同态映射，所以有

$$\varphi(x)-\varphi(y)=\varphi(x-y)=0$$

于是由核的定义推得$x-y\in \mathrm{Ker}\varphi$，而$\mathrm{Ker}\varphi=\{0\}$，所以$x-y=0$，即$x=y$。上述事实说明，若$x\neq y$，必有$\varphi(x)\neq\varphi(y)$，即$\varphi$是单射，从而证得$\varphi$是同构映射。证完。

定理 1 （环的同态基本定理）

（1）设N为环R的任一理想，则$R\overset{\varphi}{\sim}R/N$，且$\mathrm{Ker}\varphi=N$；

（2）若环R与R'同态：$R\overset{\varphi}{\sim}R'$，$N=\mathrm{Ker}\varphi$。则$R/N\cong R'$。

证明 此定理的证明与群的同态基本定理的证明完全类似，（1）的证明作为练习。下面证明（2）。

由命题 4 知$N=\mathrm{Ker}\varphi$是R的理想，再由 § 5 可知R/N有意义。规定R的商环R/N到R'的"映射"$\overline{\varphi}$如下：

$$\overline{\varphi}:\ n+N\longmapsto\varphi(x),\quad \forall x\in R$$

下面指出$\overline{\varphi}$是R/N到R'的映射。

由于R/N中的元$x+N$和$x'+N$在$x-x'\in N$时有$x+N=x'+N$。而上面所规定的$\overline{\varphi}$是根据R/N的元$x+N$的表法确定其象的，所以说明$\overline{\varphi}$是映射，需要指出：若$x+N=x'+N$，必有$\varphi(x)=\varphi(x')$。

事实上，若$x+N=x'+N$，则$x-x'\in N$。因为，$N=\mathrm{Ker}\varphi$，所以$\varphi(x-x')=0$，故$\varphi(x)=\varphi(x')$。

由上述可知$\overline{\varphi}$是映射。显然$\overline{\varphi}$是满射。下面指出$\overline{\varphi}$是单

射。$\forall\ x+N,\ y+N\in R/N$，若 $\overline{\varphi}(x+N)=\overline{\varphi}(y+N)$，则由 $\overline{\varphi}$ 的定义，$\overline{\varphi}(x+N)=\varphi(x)$，$\overline{\varphi}(y+N)=\varphi(y)$，所以有：$\varphi(x)=\varphi(y)$，即 $\varphi(x)-\varphi(y)=0$。而 $\varphi(x-y)=\varphi(x)-\varphi(y)=0$，所以 $x-y\in\mathrm{Ker}\varphi=N$。因此，$x+N=y+N$。

上述事实说明 $\overline{\varphi}$ 是单射。最后验证 $\overline{\varphi}$ 保持加法和乘法。

（1） $\overline{\varphi}((x+N)+(y+N))=\overline{\varphi}((x+y)+N)=\varphi(x+y)$
$=\varphi(x)+\varphi(y)=\overline{\varphi}(x+N)+\overline{\varphi}(y+N)$

（2） $\overline{\varphi}((x+N)(y+N))=\overline{\varphi}(xy+N)=\varphi(xy)=$
$\varphi(x)\cdot\varphi(y)=\overline{\varphi}(x+N)\overline{\varphi}(y+N)$

综上所述，$\overline{\varphi}$ 是同构映射，即 $R/N\cong R'$。证完。

环的同态基本定理与群的同态基本定理完全类似，也具有着形式简明，内容深刻的特点，对研究环的理论有着非常重要的作用。

例 $\boldsymbol{R}[x]$ 是实数域 $\boldsymbol{R}$ 上的多项式环。则

φ：$f(x)\longmapsto f(0)$，$\forall f(x)\in\boldsymbol{R}[x]$

是环 $\boldsymbol{R}[x]$ 到 $\boldsymbol{R}$ 的映射，而且是满同态，并且

$\boldsymbol{R}[x]/(x)\cong\boldsymbol{R}$

解 显然 φ 是 $\boldsymbol{R}[x]$ 到 $\boldsymbol{R}$ 的映射。而且对于 $\boldsymbol{R}$ 中任意元 a 来说，$a\in\boldsymbol{R}[x]$，

φ：$a\longmapsto a$

所以 φ 是满射。

$\forall f(x)$，$g(x)\in\boldsymbol{R}[x]$，有

$$\varphi(f(x)+g(x))=f(0)+g(0)=\varphi(f(x))+\varphi(g(x))$$
$$\varphi(f(x)\cdot g(x))=f(0)\cdot g(0)=\varphi(f(x))\cdot\varphi(g(x))$$

所以 φ 是满同态。

最后只要指出 $\mathrm{Ker}\varphi=(x)$，则由环的同态基本定理即有：$\boldsymbol{R}[x]/(x)\cong\boldsymbol{R}$。

因为，若 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，则 $f(0)=a_0$。所以，若 $f(x)\in\mathrm{Ker}\varphi$，则 $f(0)=0=a_0$。即 φ 的核中的元，其常数项 a_0 必为 0，反之，对于 $\boldsymbol{R}[x]$ 中常数项为 0 的多项式 $f(x)$

来说，必有$f(0)=0$，即$R[x]$中常数项为0的元都在φ的核中。

综上所述，可知

$\mathrm{Ker}\varphi=(x)=\{g(x)x\mid g(x)\in R[x]\}$. 所以，由环的同态基本定理有

$$R[x]/(x)\cong R$$

由于$\mathrm{Ker}\varphi=(x)\neq\{0\}$，容易证明$\varphi$不是同构映射。当然，这一结论也可以由$\varphi$的规定直接看出。

为了后面章节讨论的需要，关于环的同态和同构作进一步的讨论。

定理 2 若φ是环R到环$\overline{R}$的满同态，则

（1） R的子环S在φ之下的象：$\overline{S}=\{\varphi x\mid x\in S\}$是$\overline{R}$的子环；

（2） R的理想N在φ之下的象：$\overline{N}=\{\varphi(x)\mid x\in N\}$是$\overline{R}$的理想；

（3） $\overline{R}$的子环$\overline{S}$在R中的完全原象：$S=\{x\in R\mid\varphi(x)\in\overline{S}\}$是$R$的子环；

（4） $\overline{R}$的理想$\overline{N}$在R中的完全原象：$N=\{x\in R\mid\varphi(x)\in\overline{N}\}$是$R$的理想。

证明 只证（1），其余各条作为练习。

因为S是R的子环非空，故$\overline{S}$也非空。

$\forall\ \overline{x},\ \overline{y},\in\overline{S}$，往证$\overline{x}-\overline{y}\in\overline{S}$，$\overline{x}\,\overline{y}\in\overline{S}$。

因为$\overline{S}=\{\varphi(x)\mid x\in S\}$，可知对于$\overline{x}$，$\overline{y}\in\overline{S}$，必有$x$，$y\in S$，使$\varphi(x)=\overline{x}$，$\varphi(y)=\overline{y}$，而

$$\overline{x}-\overline{y}=\varphi(x)-\varphi(y)=\varphi(x-y)$$

$$\overline{x}\,\overline{y}=\varphi(x)\varphi(y)=\varphi(xy)$$

因为S为R的子环，而x，$y\in S$，所以$x-y$，$xy\in S$。

因此，$\varphi(x-y)$，$\varphi(xy)\in\overline{S}$，即$\overline{x}-\overline{y}$，$\overline{x}\,\overline{y}\in\overline{S}$。$\overline{S}$是$\overline{R}$的子环得证，证完。

引理 若存在代数体系$\{A;\ +,\cdot\}$到集合A'的一个双射，则可在A'中规定两个代数运算：加法$\oplus$和乘法$\odot$使得

$\{A;+,\cdot\}\cong\{A';\oplus,\odot\}$.

证明 因为φ是A到A'的双射，所以 $\forall x'\in A'$，有唯一的$x\in A$，使$\varphi(x)=x'$。

在A'中规定"加法"$\oplus$和"乘法"$\odot$如下：

$$x'\oplus y'=z'=\varphi(x+y)，即x+y=z$$

$$x'\odot y'=u'=\varphi(xy)，即xy=u.$$

其中，$x'=\varphi(x)$，$y'=\varphi(y)$，$z'=\varphi(z)$，$u'=\varphi(u)$。

容易看出，上述规定是A'的两个代数运算。而且φ保持运算。证完。

定理 3 **设S是环R的子环，$\overline{S}$是一个环.如果S'与$\overline{S}$没有公共元而且$S\cong\overline{S}$（S'是S在R中的补集），则存在$\overline{S}$的扩环$\overline{R}$，使得$R\cong\overline{R}$。**

证明 设$S=\{x_S, y_S,\cdots\}$，φ是S到$\overline{S}$的同构映射。令$\varphi(x_S)=\overline{x_S}$，则$\overline{S}=\{\overline{x_S}, \overline{y_S},\cdots\}$，并且用$x$，$y$，…表示$S'$中的元，则

$$R=\{x_S, y_S, \cdots|x, y, \cdots\}$$

令

$$\overline{R}=\{\overline{x_S}, \overline{y_S}, \cdots|x, y, \cdots\}$$

则

$$\psi: x_S\longmapsto\overline{x_S}=\varphi(x_S),\quad x\longmapsto x$$

是R到$\overline{R}$的双射。

显然，ψ是R到$\overline{R}$的映射，而且是满射，下面说明ψ是单射。

对于R中任意两个不同元a和b来说，若$a,b\in S$，则$\psi(a)=\varphi(a)$，$\psi(b)=\varphi(b)$，

因为φ是同构映射，所以$\varphi(a)\neq\varphi(b)$，即$\psi(a)\neq\psi(b)$。

若a，$b\in S'$，则$\psi(a)=a$，$\psi(b)=b$，所以$\psi(a)\neq\psi(b)$。

上述事实说明，若a、b同属于S或S'，当$a\neq b$时，a与b在ψ之下的象不相同。

如果a和b分别属于S和S'（或S'和S），由ψ的规定，则

它们的象也分别属于$\overline{S}$和$\overline{S'}$（或S'和$\overline{S}$）．但是，S和S'没有公共元，所以在ψ之下a与b的象必不相同即ψ是单射。

综合上述，ψ是双射．于是，由引理可在$\overline{R}$中规定加法和乘法（这两个运算按引理中那样去定义）使$R\cong\overline{R}$。

最后说明，$\overline{S}$是$\overline{R}$的子环，即$\overline{R}$是$\overline{S}$的扩环。

由$\overline{R}$的具体作法知$\overline{R}\supseteq\overline{S}$，下边说明$\overline{S}$关于$\overline{R}$的运算是$\overline{R}$的子环。

已知$\overline{S}$是环，所以要说明$\overline{S}$是$\overline{R}$的子环，只须说明$\overline{R}$的加法和乘法与$\overline{S}$原来已有的加法和乘法，对$\overline{S}$的作用是相同的即可。

假定用$\oplus$和$\odot$分别表示$\overline{R}$的加法和乘法，用$+$和$\cdot$分别表示$\overline{S}$的加法和乘法．因为$S\cong\overline{S}$，所以，S的加法和乘法我们也用$+$和$\cdot$去表示。

$\forall\,\overline{x_S}$、$\overline{y_S}\in\overline{S}$，则由$\overline{S}$中元素与$S$中元素的关系，有

$$\overline{x_S}=\varphi(x_S),\quad \overline{y_S}=\varphi(y_S),\quad x_S,\ y_S\in S$$

这时，有

$$\begin{aligned}\overline{x_S}+\overline{y_S}&=\varphi(x_S)+\varphi(y_S)=\varphi(x_S+y_S)\\ \overline{x_S}\cdot\overline{y_S}&=\varphi(x_S)\cdot\varphi(y_S)=\varphi(x_S\cdot y_S)\end{aligned}\qquad(1)$$

要注意，（1）式右端的$+$和$\cdot$是S的加法和乘法。

其次，对于$\overline{R}$的加法和乘法来说，按引理证明中的规定为：$\forall\,\overline{x},\ \overline{y}\in\overline{R}$，

$$\overline{x}\oplus\overline{y}=\psi(x)\oplus\psi(y)=\psi(x+y)$$

$$\overline{x}\odot\overline{y}=\psi(x)\odot\psi(y)=\psi(xy)$$

其中$\overline{x}=\psi(x)$，$\overline{y}=\psi(y)$，x，$y\in R$。

但是，对于同构映射ψ来说，由上面的规定

$$\psi(x_S)=\varphi(x_S),\quad \forall x_S\in S$$

又因

$$\forall x_S,\ y_S\in S\Longrightarrow x_S+y_S,\ x_S\cdot y_S\in S$$

所以

$$\overline{x_S}\oplus\overline{y_S}=\psi(x_S)\oplus\psi(y_S)=\psi(x_S+y_S)$$

$$= \varphi(x_S + y_S) \tag{2}$$

$$\overline{x_S} \odot \overline{y_S} = \psi(x_S) \odot \psi(y_S) = \psi(x_S \cdot y_S)$$

$$= \varphi(x_S \cdot y_S)$$

由（1）式与（2）式可以看出，$\overline{R}$的加法和乘法对$\overline{S}$的作用与$\overline{S}$原来的加法和乘法对$\overline{S}$的作用是相同的，所以，由$\{\overline{S};\ +,\ \cdot\}$是环得知$\{\overline{S};\ \oplus,\ \odot\}$是$\{\overline{R};\oplus,\odot\}$的子环。证完。

习　　题

1　证明本节命题1，2，3。

2　证明定理2（2）—（4）。

3　证明：$a+bi \longmapsto a-bi$是复数域$\mathbf{C}$的自同构。

4　$\mathbf{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,\ b \in \mathbf{Z}\}$

$\mathbf{Z}[\sqrt{3}] = \{a+b\sqrt{3} \mid a,\ b \in \mathbf{Z}\}$

是实数域$\mathbf{R}$的两个子环。证明：$\mathbf{Z}[\sqrt{2}]$与$\mathbf{Z}[\sqrt{3}]$不同构。

5　设φ是环R到环R'的同态映射，I'是R'的理想，I是I'在R中的完全原象。证明：

$R/I \cong R'/I'$

6　$\mathbf{R}$是实数域，$a \in \mathbf{R}$。证明：$\mathbf{R}[x]/(x-a) \cong \mathbf{R}$。此处$(x-a)$是$\mathbf{R}[x]$的由$x-a$所生成的主理想。

7　$\mathbf{Q}$是有理数域，求$\mathbf{Q}[i] = \{a+bi \mid a,b \in \mathbf{Q}\}$的所有自同构。

8　设S是环R的子环，I是环R的理想。证明：

（1）$S+I = \{s+a \mid s \in S, a \in I\}$是$R$的子环，而且$I$是$S+I$的理想；

（2）$S \cap I = \{x \in R \mid x \in S且x \in I\}$是$S$的理想；

（3）$(S+I)/I \cong S/S \cap I$。

§ 7 极大理想与素理想

本节进一步研究两类特殊理想，由此给出由一个交换环得到域的方法。

定义 1 设 $N(\neq R)$ 是 R 的理想，如果除 R 和 N 本身外，没有包含 N 的理想时，即若理想 $J\supset N$，则 $J=R$，则称 N 为 R 的极大理想。

例 1 当 p 是素数时，则 (p) 是整数环 $\mathbf{Z}$ 的极大理想。

解 因 $\mathbf{Z}$ 是主理想环，所以 $\mathbf{Z}$ 的任一理想都是主理想，若 $(m)\supset(p)$，则有 $p=mq$，因 p 为素数，故有 $m=\pm p$ 或 ± 1，若 $m=\pm p$，则与 $(p)\subset(m)$ 矛盾。所以 $m=\pm 1$，由此证得 $(m)=\mathbf{Z}$。即 (p) 是整数环 $\mathbf{Z}$ 的极大理想。

定理 1 设 R 为有 1 的交换环．则 R/N 是域 $\Longleftrightarrow$ N 是 R 的极大理想。

证明 必要性．设 R/N 是域，去证 N 为 R 的极大理想。

如果 J 是 R 的理想，且 $J\supset N$ 时，则由环的同态基本定理：$R\overset{\varphi}{\sim}R/N$．这时，由 § 6 定理 2 可知，在 φ 之下 R 的理想 J 的象 $\overline{J}$ 是 R/N 的理想．因为 $J\supset N$，所以有 $a\in J$，但 $a\overline{\in}N$，因此可知 $\overline{J}$ 是 $\overline{R}=R/N$ 的非零理想．但是由 § 5 例 5 知域只有两个理想：$\{0\}$ 和它本身，所以 $\overline{J}=\overline{R}$。

下面证明 $J=R$．若 $J\neq R$，则必有 $a\in R$ 而 $a\overline{\in}J$．进一步可知 $a+N\overline{\in}\overline{J}$．否则，若 $a+N\in\overline{J}$，则有 $b\in J$，使 $a+N=b+N$ 从而有 $a-b\in N$．故有 $n\in N$ 使 $a-b=n$，即 $a=n+b$．而 $J\supset N$，$n\in N$，$b\in J$ 故 $a=n+b\in J$，与 $a\overline{\in}J$ 相矛盾。综合上述可知，$J=R$．即 N 是 R 的极大理想。

充分性．设 N 为有 1 的交换环 R 的极大理想，往证 R/N 是域．由同态基本定理，$R\sim R/N$，而 R 是有 1 的交换环，故由 § 5 命题 2 可知 R/N 也是有 1 的交换环．当 N 为 R 的极大理想时，则由定义可知 $N\neq R$，从而 $R/N\neq\{\overline{0}\}$．为了说明

R/N是域，只需证明：$\forall \overline{a}(\neq\overline{0})\in R/N$都有逆元即可。

考虑R/N的主理想：$(\overline{a})=\overline{A}$。因为$\overline{a}\neq\overline{0}$，所以$(\overline{a})$是 R/N 的非零理想。令$\overline{A}$在 R/N 中的全体原象为 A，$(R\overset{\nu}{\sim}R/N)$，则由§6定理2可知$A$是$R$的理想。由同态基本定理知$\ker\nu=N$，即 $\forall n\in N$，$\nu(n)=\overline{0}$，而$\overline{A}$是R/N的理想，所以

$$A\supseteq N$$

若 $A=N$，则$\overline{A}=\{\overline{0}\}$与$\overline{A}=(\overline{a})$不是零理想相矛盾。所以$A\supset N$。而题设$N$为$R$的极大理想，所以必有

$$A=R$$

从而有 $(\overline{a})=\nu(A)=\nu(R)=R/N$，于是对$R/N$中任一元$\overline{y}$都可写为：$\overline{y}=\overline{x}\,\overline{a}$，$\overline{x}\in R/N$。特别地，对$R/N$的单位元$\overline{1}$来说，有$\overline{r}\in R/N$使

$$\overline{r}\,\overline{a}=\overline{1}$$

上式说明，$\overline{r}$是$\overline{a}$在R/N中的逆元，故R/N是域。证完。

例2 应用定理1证明本节例1。

证明 因为Z是有1的交换环，所以只要能指出 $Z/(p)$是域，则由定理1即可知(p)是Z的极大理想。

因为，$Z_p=\{\overline{0},\ \overline{1},\ \overline{2},\ \cdots,\ \overline{p-1}\}$是有1的交换环，而且对于$\overline{a}(\neq\overline{0})\in Z_p$，则$(a,\ p)=1$。所以，由整数的性质可知，有$u$，$v\in Z$使

$$au+pv=1$$

从而有

$$\overline{au+pv}=\overline{1},\quad \overline{au}+\overline{pv}=\overline{1}$$

因为$\overline{pv}=\overline{p}\,\overline{v}=\overline{0}$，所以有：$\overline{au}=\overline{a}\,\overline{u}=\overline{1}$，即$\overline{a}$在 Z_p中有逆元。故$Z_p=Z(p)$是域。于是由定理1可知(p)是Z的极大理想。

下面再介绍另一个重要的理想，在本章§10可以看到它的作用。

定义2 若N为交换环R的理想，如果$\forall a,b\in R$，$ab\in N$

$\Longrightarrow a\in N$或$b\in N$时，则称N为R的素理想。

显然，交换环R本身作为理想是R的素理想。容易看出，若零理想是交换环R的素理想时，则R没有真零因子，反之若交换环R没有真零因子，则零理想是R的素理想。

定理 2 N是交换环R的理想。R/N没有真零因子$\Longleftrightarrow N$是R的素理想。

证明 若R/N没有真零因子时，则由上述可知$\{\overline{0}\}$是R/N的素理想。于是，$\forall a, b\in R$，若$ab\in N$，则$\overline{ab}=\overline{a}\,\overline{b}=\overline{0}$，而$\{\overline{0}\}$是素理想，所以，或$\overline{a}=\overline{0}$，或$\overline{b}=\overline{0}$，即或$a\in N$或$b\in N$。所以$N$是$R$的素理想。

反之，若N是R的素理想，如果$\overline{a}\,\overline{b}=\overline{0}$，即$\overline{ab}=\overline{0}$，从而有$ab\in N$。由$N$是素理想，故有或$a\in N$，或$b\in N$，即或$\overline{a}=\overline{0}$，或$\overline{b}=\overline{0}$。因此，$R/N$没有真零因子。证完。

推论 **在有 1 的交换环R中，极大理想N是素理想。**

证明 由定理 1，当N为R的极大理想时，则R/N是域，从而R/N没有真零因子。再由定理 2 可知N是R的素理想。

限于篇幅，对极大理想和素理想只介绍上述两个主要结果。

习 题

1 (x)是不是有理数域上的多项式环$\mathbf{Q}[x]$的极大理想？

2 对整环$\mathbf{Z}[i]=\{a+bi\mid a, b\in\mathbf{Z}\}$来说，$(1+i)$是不是$\mathbf{Z}[i]$的极大理想？

3 p为素数，(p^2)是不是整数环$\mathbf{Z}$的素理想？

4 p是素数，R是偶数环，$(2p)$是不是R的极大理想？

5 $\mathbf{Z}[x]=\{a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\mid a_i\in\mathbf{Z}, n$为非负整数$\}$是有理数域上的多项式环$\mathbf{Q}[x]$的子环。证明：$\mathbf{Z}[x]$的理想$(x)$是素理想。

6 已知$S_p=\{\frac{a}{b}\in\mathbf{Q}\mid a, b\in\mathbf{Z}, p\nmid b\}$（$p$是素数）是整环，证明，$(p)$是$S_p$的极大理想而且是素理想。

7　设N是R的理想，N'是N在R中的补集.证明：N是R的素理想必要而且只要N'关于R的乘法是半群.

8　证明：$M_2(\mathbf{Q})$只有平凡（当然）理想，但不是除环.

§8　商　　域

上节定理1给出了一个由已知有1的交换环构造域的方法，本节将给出由一个整环构造域的方法.

我们知道，除环的任意子环都没有真零因子，那么每一个没有真零因子的环能否嵌入一个除环？这句话的含意是：给定一个没有真零因子的环S，存在不存在S到某一除环D里的一个单同态映射？如果存在S到某一除环D里的一个单同态映射，那么S将同构于D的子环$\overline{S}$，于是S与$\overline{S}$即可看作是一样的，从而可把S看作除环D的一个子环.

这个问题在相当一段时期没有解决，直到1936年马尔采夫（А，И，Мальцев）给出了一个不能嵌入一个除环的非交换无真零因子的环的例子，这个问题才得到否定的回答.

但是对于每个没有真零因子的交换环来说，却能作到这一点，即，每个没有真零因子的交换环都能嵌入到一个域中，本节将给出这个结果.解决这一问题所用到的方法，恰好是由整数环构造有理数域的方法.

定理1　**任意没有真零因子的交换环S都能嵌入到一个域中.**

在证明定理1之前，先研究一下一个域K的子环S和由S所生成的（K的）子域F之间的关系.

为此，先考察一下由S所生成的域F中元的形式.显然，$\forall a$，$b(\neq 0)\in S$，则$ab^{-1}\in F$.由此可见，F至少必须包含一切形如ab^{-1}的元素，$\forall a$，$b(\neq 0)\in S$.事实上，F恰是一切这样元素所构成的.

这是因为，$\forall a$，$b(\neq 0)$，c，$d(\neq 0)\in S$.

$$ab^{-1}+cd^{-1}=adb^{-1}d^{-1}+cbb^{-1}d^{-1}=(ad+bc)b^{-1}d^{-1}$$
$$=(ad+bc)(bd)^{-1}$$
$$0=0b^{-1},\quad -(ab^{-1})=(-a)b^{-1}$$
$$(ab^{-1})(cd^{-1})=acb^{-1}d^{-1}=(ac)(bd)^{-1}$$
$$1=aa^{-1},\quad (ab^{-1})^{-1}=ba^{-1},\ \text{当}a\neq 0$$

上列各式表明，形如ab^{-1}这样的元素之和、积、零元、负元、单位元、逆元等也是形如ab^{-1}这种形的元素。所以，域K的子集$\{ab^{-1}|a,\ b\in S,\ b\neq 0\}$是$K$的子域．（应该注意到，此处用到了乘法的交换性）．

另一方面，S中的元a都可写为：$a=a1^{-1}$，所以S被K的子域$\{ab^{-1}|a,\ b\in S,\ b\neq 0\}$包含．因为由$S$所生成的域$F$没有包含$S$的真子域，所以$F=\{ab^{-1}|a,\ b\in S,\ b\neq 0\}$。

还须说明的是，由S所生成的子域中的元，当且仅当$ad=bc$时，$ab^{-1}=cd^{-1}$。这是因为，若$ab^{-1}=cd^{-1}$，则用bd乘它们两边，即有

$$ad=bc$$

反之，若$ad=bc$时，则用$b^{-1}d^{-1}$乘它们的两边，即有

$$ab^{-1}=cd^{-1}$$

下面来证明定理1．若S只含零元，则定理1显然成立。若$S\neq\{0\}$，这时S的非零元的集合$\dot{S}\neq\phi$。考虑S与$\dot{S}$的笛卡尔积

$$S\times\dot{S}=\{(a,b)|a\in S,\ b\in\dot{S}\}$$

在$S\times\dot{S}$中规定一个关系"$\sim$"

$$(a,\ b)\sim(c,\ d)\Longleftrightarrow ad=bc$$

下面指出关系"$\sim$"是等价关系。

（1）因为$ab=ba$所以$(a,\ b)\sim(a,\ b)$；

（2）若$(a,\ b)\sim(c,\ d)$则$ad=bc$，于是有$cb=da$，所以有$(c,\ d)\sim(a,\ b)$；

（3）若$(a,\ b)\sim(c,\ d)$，$(c,\ d)\sim(e,\ f)$

则有$ad=bc$，$cf=de$，于是有

$$adf = bcf = bde$$

因为 $d \neq 0$，且 S 是没有真零因子的交换环，所以由 $adf = bde$ 可消去 d，得到 $af = be$，于是有

$$(a,\ b) \sim (e,\ f)$$

综合上述，得知"$\sim$"是等价关系。

现在令 $\frac{a}{b}$ 表示 (a,b) 由"$\sim$"所确定的类，并把它叫做分式（商）。由关系"$\sim$"可知

$$\frac{a}{b} = \frac{c}{d} \Longleftrightarrow ad = bc$$

令 $F = \{\frac{a}{b} \mid a \in S, b \in \dot{S}\}$ 是 $S \times \dot{S}$ 由等价关系"$\sim$"所确定的商集。在 F 中规定"加法"和"乘法"

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \frac{c}{d} = \frac{ac}{bd}$$

下面验证上述规定都是 F 的代数运算。因为 S 中没有真零因子，故由 b，$d \in \dot{S}$，即 $b \neq 0$，$d \neq 0$，推出 $bd \neq 0$，即 $bd \in \dot{S}$。因此 $\frac{ad + bc}{bd}$，$\frac{ac}{bd}$ 都是 F 中的元。

其次说明，上述规定与类的代表选择无关。若 $\frac{a}{b} = \frac{a'}{b'}$，$\frac{c}{d} = \frac{c'}{d'}$ 往证：$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{b'}$，即 $\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}$ 和 $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ 成立。

若 $\frac{a}{b} = \frac{a'}{b'}$，$\frac{c}{d} = \frac{c'}{d'}$，则有

$$ab' = a'b,\quad cd' = c'd$$

因为

$$(ad+bc)b'd' = (ab')dd' + bb'(cd')$$
$$= (a'b)dd' + bb'(c'd)$$
$$= (a'd' + b'c')bd$$
$$(ac)b'd' = (ab')(cd') = a'bc'd = (a'c')bd$$

所以有

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'},\quad \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

上述说明，上述规定与类的代表的选择无关，所以是 F 的代数运算。

下面验证代数体系 $\{F;\ +,\ \cdot\}$ 是域。

（1）$\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$；

（2）$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf+de}{df} = \frac{adf+bcf+bde}{bdf}$，

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf+bcf+bde}{bdf}；$$

（3）$\frac{0}{b} + \frac{c}{d} = \frac{bc}{bd} = \frac{c}{d}$；

（4）$\frac{a}{b} + \frac{-a}{b} = \frac{0}{b}$。

综合（1）～（4）可知 $\{F;\ +\}$ 是加群。

同样可以验证，F 的乘法满足交换律和结合律，乘法对加法的分配律；$\frac{b}{b}$ 是单位元，$\frac{a}{b}$ 的逆元是 $\frac{b}{a}$。所以 $\{F;\ +,\ \cdot\}$ 是域。令

$$\overline{S} = \left\{\frac{ab}{b} \in F \mid b \text{ 为 } S \text{ 中固定元，} a \in S\right\}$$

则

$$\varphi:\ a \longmapsto \frac{ab}{b}$$

是 S 到 $\overline{S}$ 的双射。而且

$$\varphi(a+a')=\frac{(a+a')b}{b}=\frac{ab+a'b}{b}=\frac{ab}{b}+\frac{a'b}{b}$$

$$=\varphi(a)+\varphi(a')$$

$$\varphi(aa')=\frac{aa'b}{b}=\frac{aa'b^2}{b^2}=\frac{ab}{b}\cdot\frac{a'b}{b}$$

$$=\varphi(a)\varphi(a')$$

所以 $S\cong\overline{S}$. 于是由本章§6定理3，存在一个包含 S 的域 Q，证完。

在上面的证明中，我们看到，域 Q 与环 S 的关系正相当于整数环与有理数域的关系. 事实上，上述的作法正是套用由整数环构造有理数域的方法。

定义 一个域 Q 如果包含环 S，而且

$$Q=\left\{\frac{a}{b}=ab^{-1}\mid a,\ b(\neq 0)\in S\right\}$$

则称 Q 为 S 的商域（分式域）.

由定理1可知，任一没有真零因子的交换环至少有一个商域存在。

定理2 若环 R 至少含两个元，而 F 是含 R 的域，则 F 必包含 R 的一个商域。

证明 在 F 中

$$ab^{-1}=b^{-1}a=\frac{a}{b}\ (a,\ b\in R,\ b\neq 0)$$

有意义，则F的子集

$$\overline{Q}=\left\{\frac{a}{b}\mid a,\ b(\neq 0)\in R\right\}$$

显然是 R 的商域。证完。

由于环 R 的每一个商域都必满足规则

$$\frac{a}{b}=\frac{c}{d}\Longleftrightarrow ad=bc$$

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

而上述这些规则完全由环R的加法和乘法所决定，因此，环R的商域的构造完全由R决定。所以有

定理 3　同构的环的商域必同构。

习　　题

1　求$\mathbf{Z}[i]=\{a+bi|a, b\in\mathbf{Z}\}$的商域。

2　$\mathbf{R}$是实数域，求$\mathbf{R}[x]$的商域。

3　设p是素数。求$S_p=\{\frac{a}{b}|a, b\in\mathbf{Z}, p\nmid b\}$的商域。

4　证明：域F是它自身的商域。

§9　多项式环

以前我们所接触到的多项式，它的系数都是实数和复数或更一般的是数域中的数，现在把它推广到一般情形。

设R_0是一个有1的交换环，R是R_0的子环并且包含R_0的单位元1。

定义 1 *　$\alpha\in R_0$，R_0 **中形如**

$f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n$，$a_i\in R$，（$n$ **是非负整数**）

的元，叫做R上的α的多项式，a_i叫做多项式$f(\alpha)$的系数。

下面来考虑R上的α的多项式的集合

$R[\alpha]=\{a_0+a_1\alpha+\cdots+a_n\alpha^n|a_i\in R$，$n$是任意非负整数$\}$

通过验算可知，R上的α的多项式的集合$R[\alpha]$是R_0的包含R和α的子环。

事实上

$\forall f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n$,

$g(\alpha)=b_0+b_1\alpha+\cdots+b_m\alpha^m\in R[\alpha]$

---

* 参看本节学习指导的补充说明。

若$m<n$，则可将$g(\alpha)$写为

$$g(\alpha)=b_0+b_1\alpha+\cdots+b_m\alpha^m+0\alpha^{m+1}+\cdots+0\alpha^n$$

于是

$$f(\alpha)+g(\alpha)=(a_0+b_0)+(a_1+b_1)\alpha+\cdots+(a_m+b_m)\alpha^m+(a_{m+1}+0)\alpha^{m+1}+\cdots+(a_n+0)\alpha^n$$

$$f(\alpha)\cdot g(\alpha)=(a_0+a_1\alpha+\cdots+a_n\alpha^n)(b_0+b_1\alpha+\cdots+b_m\alpha^m)$$
$$=c_0+c_1\alpha+\cdots+c_k\alpha^k+\cdots+c_{n+m}\alpha^{n+m}$$

其中 $c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0=\sum\limits_{i+j=k}a_ib_j$，而且

$$-f(\alpha)=(-a_0)+(-a_1)\alpha+\cdots+(-a_n)\alpha^n\in R[\alpha]$$

综合上述，$R[\alpha]$是R_0的子环，至于$R[\alpha]$包含α和R是显然的。而且容易看出$R[\alpha]$是包含R和α的R_0的最小子环。

为叙述方便我们称$R[\alpha]$为R上的α的多项式环。对于R_0中的元素α来说，当$f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n$的系数不全为0时，有可能$f(\alpha)=0$，例如，当$\alpha=a\in R$时，则取$a_0=a$，$a_1=-1$（1为$R_0$的单位元），则多项式

$$a_0+a_1\alpha=a-a=0$$

定义 2 环R_0的一个元x，叫做R上的一个未定元，如果对于$R[x]$中的任一多项式$f(x)$有：若$f(x)=a_0+a_1x+\cdots+a_nx^n=0$，必须$a_0=a_1=\cdots=a_n=0$。

本节主要讨论未定元x的多项式。

据根定义2，R上的未定元x的多项式（简称为一元多项式）只能用一种方法写为

$$a_0+a_1x+\cdots+a_nx^n\quad(a_i\in R)$$

的形式（不计系数是0的项）。

关于一元多项式，可以象数域上的多项式那样引进次数的概念。

定义 3 $f(x)=a_0+a_1x+\cdots+a_nx^n$，$a_n(\neq0)\in R[x]$，则称$n$为$f(x)$的次数，记作：$\deg f(x)=n$，$a_nx^n$叫做$f(x)$的首项。零多项式（即系数都是0的多项式）不定义次数。

容易看出，当 $f(x)+g(x)\neq 0$，$f(x)g(x)\neq 0$时，则

（1）$\deg(f(x)+g(x))\leqslant\max(\deg f(x),\ \deg g(x))$

（2）$\deg(f(x)g(x))\leqslant\deg f(x)+\deg g(x)$

而且，当R是整环时，（2）式的等号成立。

对于给定的有1的交换环R_0来说，是否一定存在R上的未定元x？下面来回答这一问题。

定理1　若R是有1的交换环，则存在R的扩环 R_0，在R_0中存在R上的未定元x，从而对任意有1的交换环R来说，存在一元多项式环 $R[x]$。

证明　下面先来构造R的一个扩环P。而P是一个与R有相同的单位元的交换环，然后再指出在P中存在R上的未定元x。

1　先构造R的扩环P。

令　$\overline{P}=\{(a_0,\ a_1,\ a_2,\ \cdots)\,|\,a_i\in R$，只有有限个$a_i\neq 0\}$。规定：$(a_0,\ a_1,\ a_2,\ \cdots)=(b_0,\ b_1,\ b_2,\ \cdots)\Longleftrightarrow a_i=b_i$，$i=0,\ 1,\ 2,\cdots$。

在$\overline{P}$中规定加法和乘法如下：

$$(a_0,a_1,a_2,\cdots)+(b_0,b_1,b_2,\cdots)=(a_0+b_0,\ a_1+b_1,\ a_2+b_2,\ \cdots)$$

$$(a_0,a_1,a_2,\cdots)\cdot(b_0,b_1,b_2,\cdots)=(c_0,c_1,c_2,\cdots)$$

其中，$c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0$，$k=0,\ 1,\ 2,\ \cdots$。

显然，上述规定是$\overline{P}$的代数运算。由于$\overline{P}$中的元：$(a_0,\ a_1,\ a_2,\ \cdots,\ a_n,\ \cdots)$中只能有有限个 $a_i\neq 0$，所以，把它和一元多项式

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$$

联系起来看（假定存在R上的未定元x），上面对$\overline{P}$所定义的加法和乘法，其实就是多项式的加法和乘法。

按照上述规定和环R的性质，可以验证：

（1）$\overline{P}$的加法满足交换律和结合律；

（2）$\overline{P}$的乘法满足交换律和结合律；

（3）$\overline{P}$的乘法对加法满足分配律；

（4）$(0,0,\cdots,0,\cdots)$ 是$\overline{P}$的加法恒等元，即零元；

（5）$(a_0,a_1,a_2,\cdots)$在$\overline{P}$中的负元是$(-a_0, -a_1, -a_2, \cdots)$；

（6）$(1, 0, 0,\cdots)$是$\overline{P}$的单位元

综合上述，$\overline{P}$是有1的交换环。其次应用上面所得到的环$\overline{P}$，构造一个包含环R的扩环。由于

$$(a, 0, 0, \cdots)+(b, 0, 0, \cdots)=(a+b, 0, 0, \cdots)$$

$$(a, 0, 0, \cdots)\cdot(b, 0, 0, \cdots)=(ab, 0, 0, \cdots)$$

所以$\overline{P}$的子集

$$\overline{R}=\{(a, 0, 0, \cdots)\ |a\in R\}$$

是$\overline{P}$的子环，而且

$$(a, 0, 0, \cdots)\longmapsto a$$

是$\overline{R}$到R的一个同构映射。因为R与$\overline{P}$没有公共元，所以由本章§6定理3，用R代替$\overline{R}$而得到一个包含R的环P。这时P也是有1的交换环，而且P的单位元就是R的单位元。

2　最后指出P包含R上的未定元x，把P中的元：$(0,1, 0, \cdots)$用x表示

$$x=(0, 1, 0, \cdots)$$

下面证明x是R上的未定元。首先

$$x^2=(0, 0, 1, 0, \cdots)$$

$$x^3=(0, 0, 0, 1, 0, \cdots)$$

$$\vdots$$

$$x^k=(\underbrace{0, \cdots, 0}_{k\text{个}}, 1, 0, \cdots)\quad(k=1, 2, \cdots)$$

在P中若

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n=0,\quad a_i\in R$$

则在$\overline{P}$中有

$$(a_0,0,\cdots)+(a_1,0,\cdots)x+\cdots+(a_n,0,\cdots)x^n$$
$$=(0, 0, \cdots)$$

即 $$(a_0,0,\cdots)+(a_1,0,\cdots)(0,1,0,\cdots)+\cdots+(a_n,0,\cdots)(\underbrace{0,\cdots0}_{n\text{个}},1,0,\cdots)$$

$$=(0,0,\cdots)$$

$$(a_0,0,\cdots)+(0,a_1,0,\cdots)+\cdots+(0,\cdots,0,a_n,0,\cdots)$$

$$=(0,0,\cdots)$$

于是有

$$(a_0,a_1,\cdots,a_n,0,\cdots)=(0,0,\cdots)$$

所以 $a_i=0$，$i=0,1,2,\cdots,n$. 上述说明，$x=(0,1,0,\cdots)$是R上的未定元，证完。

由前边的讨论可知，$R[x]$是有1的交换环，而且它的单位元就是交换环R的单位元。这样一来，就可以在一元多项式环的基础上建立n元多项式环的理论。

设R_0是有1的交换环，R是R_0的子环并且包含R_0的单位元1. 设$\alpha_1,\alpha_2,\cdots,\alpha_n$是$R_0$中$n$个元，则可以作$R$上的$\alpha_1$的多项式环$R[\alpha_1]$，然后作$R[\alpha_1]$上的$\alpha_2$的多项式环$R[\alpha_1][\alpha_2]$。继续下去，可以得到多项式环$R[\alpha_1][\alpha_2]\cdots[\alpha_n]$。这个环是$R_0$的子环，它是由$R_0$中一切形如：

$$\sum a_{i_1i_2\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n} \qquad (*)$$

的元构成的。其中，$a_{i_1i_2\cdots i_n}\in R$且只有有限个不为0.

定义 4 R_0中形如$(*)$的元叫做R上的$\alpha_1,\alpha_2,\cdots,\alpha_n$的多项式，$a_{i_1i_2\cdots i_n}$叫做多项式的系数。

多项式环$R[\alpha_1][\alpha_2]\cdots[\alpha_n]$叫做$R$上的$\alpha_1,\alpha_2,\cdots,\alpha_n$的多项式环，用符号$R[\alpha_1,\alpha_2,\cdots,\alpha_n]$* 表示。

与一元多项式环类似，有

定义 5 R_0的n个元$x_1,x_2,\cdots,x_n$，叫做R上的无关未定

---

* 参阅本章§3习题5.

元，如果对于$R[x_1,x_2,\cdots,x_n]$中任一多项式$f(x_1,x_2,\cdots,x_n)=0$，必须$f(x_1,x_2,\cdots,x_n)$的所有系数都等于0.

应用定理1作数学归纳法我们有

定理2 设R是一个有1的交换环，对任意正整数n，一定有R上的n个无关未定元$x_1,x_2,\cdots,x_n$存在，从而存在R上的多项式环$R[x_1,x_2,\cdots,x_n]$。

证明从略。

定理3 设$R[x_1,x_2,\cdots,x_n]$和$R[\alpha_1,\alpha_2,\cdots,\alpha_n]$都是有1交换环$R$上的多项式环。则$R[x_1,x_2,\cdots,x_n]$与$R[\alpha_1,\alpha_2,\cdots,\alpha_n]$同态。其中，$x_1,x_2,\cdots,x_n$是$R$上的无关未定元，$\alpha_1,\alpha_2,\cdots,\alpha_n$是$R$的扩环$R_0$中的任意元。

证明 设

$$f(x_1,x_2,\cdots,x_n)=\sum a_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$$

$$f(\alpha_1,\alpha_2,\cdots,\alpha_n)=\sum a_{i_1i_2\cdots i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n}$$

由于$x_1,x_2,\cdots x_n$是R上的无关未定元，所以$f(x_1,x_2,\cdots,x_n)$中的系数$a_{i_1i_2\cdots i_n}$唯一确定。则

$$f(x_1,x_2,\cdots,x_n)\longmapsto f(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

是$R[x_1,x_2,\cdots,x_n]$到$R[\alpha_1,\alpha_2,\cdots,\alpha_n]$的映射。显然此映射是满射。

由于在$R[x_1,x_2,\cdots,x_n]$和在$R[\alpha_1,\alpha_2,\cdots,\alpha_n]$中二多项式相加或相乘是适合同一规定律的，所以上述满射是同态映射。证完。

习　　题

1　令$R=\mathbf{Z}_6$，

$f(x)=\bar{3}x^3+\bar{5}x+\bar{2}$，$g(x)=\bar{4}x^2+\bar{5}x+\bar{3}\in\mathbf{Z}_6[x]$

（1）计算　$f(x)g(x)$和$f(x)-g(x)$；

（2）求　$f(x)g(x)$的次数。

2　若x是R上的未定元，则x^k也是R上的未定元$(k\geqslant 1)$。此处R是有1的交换环。

3　证明：一元多项式环$R[x]$能与它的真子环同构。

4　设 I 是整环，Q是 I 的商域。证明：I 上的未定元x也是Q 上的未定元。

5　证明：

（1）$R[a_1,a_2]=R[a_2, a_1]$；

（2）若$x_1,x_2,\cdots,x_n$是R上的无关未定元，则每个 x_i都是R上的未定元。

6　若$x_1,x_2, \cdots, x_n$和$y_1, y_2,\cdots,y_n$是R上的两组无关未定元。则

$$R[x_1x_2,\cdots x_n]\cong R[y_1,y_2,\cdots,y_n]$$

§10　整环和域上的多项式环

本节介绍关于整环和域上的一元多项式环的进一步结果。

设 I 是整环，x是 I 上的未定元。

定理1　整环 I 上的一元多项式环$I[x]$也是整环。

证明　由上节的讨论已知$I[x]$是有1的交换环，所以只需证明 $I[x]$没有真零因子即可。设

$$f(x)=a_0+a_1x+\cdots+a_nx^n,\ a_n\neq 0$$

$$g(x)=b_0+b_1x+\cdots+b_mx^m,\ b_m\neq 0$$

是$I[n]$中任意二非零元。因为 I 是整环，所以由 $a_n\neq 0$， $b_m\neq 0$有$a_nb_m\neq 0$。而

$$f(x)g(x)=a_0b_0+\cdots+a_nb_mx^{n+m}$$

所以$f(x)g(x)\neq 0$，因此，$I[x]$没有真零因子，即$I[x]$是整环。证完。

推论1　若　$f(x)(\neq 0)$，$g(x)(\neq 0)\in I[x]$，则

$$\deg(f(x)g(x))=\deg f(x)+\deg g(x)$$

定义1　$f(x)$，$g(x)\in I[x]$，如果在$I[x]$中存在$q(x)$，使得：$f(x)=g(x)q(x)$，则说$g(x)$整除$f(x)$，记作：$g(x)\mid f(x)$；否则，就说$g(x)$不能整除$f(x)$，记作：$g(x)\nmid f(x)$。

当$g(x)\mid f(x)$时，$g(x)$叫做 $f(x)$的因子。

定理 2 若 $f(x)$，$g(x)(\neq 0)\in I[x]$，且 $g(x)$ 的首项系数为 I 中的单位（可逆元），则在 $I[x]$ 中存在唯一一对多项式 $q(x)$ 和 $r(x)$ 使

$$f(x)=g(x)q(x)+r(x)$$

其中，$r(x)=0$ 或 $\deg r(x)<\deg g(x)$。

此定理中的 $q(x)$ 叫做 $g(x)$ 除 $f(x)$ 所得到的商式，$r(x)$ 叫做 $g(x)$ 除 $f(x)$ 所得到的余式。定理 2 的证明与数域 F 上的多项式环的带余除法定理的证明完全类似，作为练习请读者自己证明。

推论 2 若 $g(x)$ 的首项系数是 I 中的单位．$g(x)\mid f(x)$ 必要而且只要 $g(x)$ 除 $f(x)$ 所得的余式等于0。

定义 2 若 $c\in I$，$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in I[x]$。则 $f(c)=a_nc^n+a_{n-1}c^{n-1}+\cdots+a_1c+a_0$ 叫做 $f(x)$ 在 $x=c$ 时的值，当 $f(c)=0$ 时，则 c 叫做 $f(x)$ 的根或零点。

由 § 9 定理 3 可知，若

$$f(x)+g(x)=h(x),\quad f(x)g(x)=k(x)$$

则 $f(c)+g(c)=h(c)$，$f(c)g(c)=k(c)$。

定理 3 $f(x)\in I[x]$，则 $x-c$ 除 $f(x)$ 的余式为 $f(c)$。

证明 由定理 2 有 $q(x)$ 和 $r(x)$，使

$$f(x)=(x-c)q(x)+r(x)$$

若 $r(x)\neq 0$，则 $\deg r(x)<1$。于是可知 $r(x)=r\in I$。即

$$f(x)=(x-c)q(x)+r$$

所以有 $f(c)=(c-c)q(c)+r=r$。证完。

由推论 2 和定理 3 则有

推论 3 $c\in I$ 是 $f(x)\in I[x]$ 的根，必要而且只要 $x-c\mid f(x)$。

设 c 是 $f(x)\in I[x]$ 的根，如果存在正整数 k，使得：$(x-c)^k\mid f(x)$，但 $(x-c)^{k+1}\nmid f(x)$，则称 c 为 $f(x)$ 的 k 重根，k 叫做根 c 的重数。当 $k>1$ 时，则 c 叫做 $f(x)$ 的重根。

由于 $I(x)$ 是整环，所以当 c_1，c_2，$\cdots$，c_r 是 $f(x)$ 的所有不同的根，并且各根的重数分别为：k_1，k_2，$\cdots$，k_r 时，则有

$(x-c_1)^{k_1}(x-c_2)^{k_2}\cdots(x-c_r)^{k_r}\mid f(x)$。

这一结论的证明作为练习。于是有

$$k_1+k_2+\cdots+k_r\leqslant\deg f(x)$$

上式说明，n 次多项式$f(x)$的根的个数（k 重根按 k 个计算）不超过$f(x)$的次数，即$f(x)$在 I 中至多有 n 个根。

至于$I[x]$中的元$f(x)$是否有重根，可以给出相当于数域上多项式环的结果。为此引进下面的定义。

定义 3 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0\in I[x]$，则

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+2a_2x+a_1$$

叫做$f(x)$的（一阶）导数。

由导数定义可直接验证导数满足下列规则：

（1）$(f(x)+g(x))'=f'(x)+g'(x)$

（2）$(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)$

（3）$(f^k(x))'=kf^{k-1}(x)f'(x)$

作为练习请读者自己验证

定理 4 c 是$f(x)$的重根必要而且只要，$x-c\mid f(x),f'(x)$。

证明 必要性。若 c 是 $f(x)$ 的重根，则 $x-c\mid f(x)$，且有

$$f(x)=(x-c)^kg(x)\quad(k>1)$$

于是由规则（2）和（3）有

$$\begin{aligned}f'(x)&=k(x-c)^{k-1}g(x)+(x-c)^kg'(x)\\&=(x-c)^{k-1}[kg(x)+(x-c)g'(x)]\end{aligned}$$

因为$k>1$，所以 $k-1\geqslant1$，故有 $x-c\mid f'(x)$。

充分性。若$x-c\mid f(x)$，$x-c\mid f'(x)$。如果c不是$f(x)$的重根，则$f(x)=(x-c)g(x)$，这时$x-c\nmid g(x)$。即 $g(c)\neq0$。而

$$f'(x)=g(x)+(x-c)g'(x)$$

所以，$f'(c)=g(c)+(c-c)g'(c)=g(c)\neq0$。于是由推论 3 得到：$x-c\nmid f'(x)$，与$x-c\mid f'(x)$相矛盾。所以，$c$ 是$f(x)$的重根。证完。

当 I 是域 F 时，则因域中任意非零元都是单位（可逆

元），所以定理 2 对$F[x]$中任意二多项式$f(x)$和$g(x)\neq 0$ 都成立：即，在$F[x]$中存在唯一一对多项式：$q(x)$，$r(x)$使

$$f(x)=g(x)q(x)+r(x)$$

其中，$r(x)=0$或 $\deg r(x)<\deg g(x)$，由此，对域F上的多项式环$F[x]$可以得到下面的重要结果。

定理 5　$F[x]$ 是主理想环。

证明　根据主理想环的定义，要证$F[x]$是主理想环，只须证$F[x]$中任一理想J都是主理想即可。

若$J=\{0\}$，显然 J 是主理想。

若$J\neq\{0\}$，则在 J 中存在非零多项式。令$p(x)$为 J 中次数最低的元，且设 $\deg p(x)=p$。

则由 $p(x)$所生成的主理想$(p(x))\subseteq J$。

另一方面，对于 J 中任意元$f(x)$来说，由定理 2 可知，存在 $q(x)$ 和 $r(x)$ 使

$$f(x)=p(x)q(x)+r(x)$$

其中，$r(x)=0$，或$\deg r(x)<\deg p(x)$。

因为 J 是$F[x]$的理想，所以$r(x)=f(x)-p(x)\cdot q(x)\in J$。如果$r(x)\neq 0$，则与 $p(x)$是 J 中次数最低的元相矛盾。所以，上式中的 $r(x)$必须为 0，即

$$f(x)=p(x)q(x)$$

上式表明，$f(x)\in(p(x))$。即 J 中任意元$f(x)$ 都在$(p(x))$中。所以 $J=(p(x))$。

综上所述，可知 $F[x]$中任一理想都是主理想，从而 $F[x]$是主理想环，证完。

定理 6　设F为域，$f(x)$ 和 $g(x)$是 $F[x]$中两个不全为 0 的元。如果$d(x)\mid f(x),g(x)$（$d(x)$叫做$f(x)$与$g(x)$的公因子），而且$d(x)$是 $f(x)$与 $g(x)$的公因子中次数最大的元，则 $d(x)$是 $F[x]$ 的理想：

$$J=\{f(x)u(x)+g(x)v(x)\mid u(x),\ v(x)\in F[x]\}$$

中次数最小的一个元，并且 $J=(d(x))$，从而在 $F[x]$ 中存在

$u_0(x)$，$v_0(x)$，使得：

$$f(x)u_0(x)+g(x)v_0(x)=d(x)$$

证明 由题设$f(x)$和$g(x)$不全为0，所以$F(x)$的理想$J\neq\{0\}$。设$p(x)$是J中次数最小的元。则由定理5的证明可知：$J=(p(x))$。

如果能证得：$p(x)=cd(x)$，$c(\neq 0)\in F$，则有

（1）$d(x)=c^{-1}p(x)$从而有$(d(x))=(p(x))=J$；

（2）$\deg p(x)=\deg c+\deg d(x)=0+\deg d(x)=\deg d(x)$，

即$d(x)$是J中次数最小的多项式。

（1）和（2）说明定理6成立。

下面证：$p(x)=cd(x)$，$c(\neq 0)\in F$。因为

$$f(x)=f(x)\cdot 1+g(x)\cdot 0,\quad g(x)=f(x)\cdot 0+g(x)\cdot 1$$

所以$f(x)$，$g(x)\in J$，而$J=(p(x))$。故有

$$f(x)=p(x)q_1(x),\quad g(x)=p(x)q_2(x),$$
$$q_1(x),\quad q_2(x)\in F[x]$$

即$p(x)\mid f(x)$，$p(x)\mid g(x)$。

由题设，$d(x)$是$F[x]$中能同时整除$f(x)$和$g(x)$的元中次数最大的，所以有：$\deg d(x)\geqslant\deg p(x)$。

另一方面，因为$p(x)=f(x)u_1(x)+g(x)v_1(x)$，而且，$d(x)\mid f(x)$，$g(x)$。所以$d(x)\mid p(x)$，即$p(x)=d(x)q(x)$。

因为$p(x)$和$d(x)$都不能为0，所以

$$\deg p(x)\geqslant\deg d(x)$$

上述已证得：$\deg d(x)\geqslant\deg p(x)$，所以有

$$\deg p(x)=\deg d(x)$$

但由$p(x)=d(x)q(x)$有

$$\deg p(x)=\deg d(x)+\deg q(x)$$

故有$\deg q(x)=0$，即$q(x)$为$F[x]$中的0次多项式，即$q(x)=c(\neq 0)\in F$，所以有：$p(x)=cd(x)$，$(c\neq 0)\in F$。因此有

$$(d(x))=(p(x))=J$$

$= \{f(x)u(x)+g(x)v(x) \mid u(x), v(x) \in F[x]\}$

显然，在 $F[x]$中存在$u_0(x)$，$v_0(x)$使

$$f(x)u_0(x)+g(x)v_0(x)=d(x)$$

至于$d(x)$是 J 中次数最小的元，在上面已作了说明，于是定理 6 得到证明。证完。

定义 4　I 是整环，x 是 I 上的未定元，$f(x)$ 是 $I[x]$中次数大于0的元，如果$f(x)$能表为 $I[x]$中两个次数都小于 $f(x)$ 的元 $f_1(x)$ 和$f_2(x)$之积：$f(x)=f_1(x)f_2(x)$，则 $f(x)$ 叫做 I 上的可约多项式。否则，即$f(x)$不能表为次数都小于$f(x)$的次数的二多项式之积时，则$f(x)$叫做 I 上的不可约多项式。

容易知道，$f(x)$ 是 I 上的不可约多项式时，如果 $f(x)=f_1(x)f_2(x)$，则 $f_1(x)\in I$ 或 $f_2(x)\in I$。反之，对于次数大于0的多项式$f(x)$来说，如果$f(x)=f_1(x)f_2(x)$必有：$f_1(x)\in I$或$f_2(x)\in I$时，则 $f(x)$必为 I 上的不可约多项式。

对于域F上的多项式环中的不可约多项式，有

定理 7　$p(x)\in F[x]$是 F 上的不可约多项式，如果 $p(x)\mid f(x)g(x)$，则 $p(x)\mid f(x)$ 或者 $p(x)\mid g(x)$。其中，$f(x)$，$g(x)\in F[x]$。

证明　若$p(x)\nmid f(x)$，这时同时整除$p(x)$和 $f(x)$的元必为 $F[x]$ 中的0次多项式。否则，若 $d(x) \mid p(x)$，$f(x)$，而且 $\deg d(x)>0$时，则有：$p(x)=d(x)q(x)$。

因为 $p(x)$为不可约多项式，而且假定 $\deg d(x)>0$，所以有$q(x)\in F$，因 $p(x)\neq 0$故 $q(x)\neq 0$，即 $q(x)$ 是域F中的非零元：$q(x)=c(\neq 0)\in F$。

所以，由$p(x)=d(x)\cdot c$ 有 $d(x)=c^{-1}p(x)$，

因为 $d(x)\mid f(x)$，所以 $c^{-1}p(x)\mid f(x)$，故有 $p(x)\mid f(x)$ 与 $p(x)\nmid f(x)$ 相矛盾。

由上述可知，若 $p(x)\nmid f(x)$，则 1 （F 的单位元）是同时整除 $p(x)$ 和 $f(x)$ 的元中次数最大的元。于是由定理 6，在 $F[x]$ 中存在 $u(x)$和 $v(x)$使，

$$f(x)u(x)+p(x)v(x)=1$$

用$g(x)$乘上式两边，则有

$$(f(x)g(x))u(x)+p(x)((v(x)g(x))=g(x)$$

因为已知$p(x)\mid f(x)g(x)$，所以有 $q(x)\in F[x]$使

$$f(x)g(x)=p(x)q(x)$$

于是得到

$$(p(x)q(x))u(x)+p(x)(v(x)g(x))=g(x)$$

即 $p(x)[q(x)u(x)+v(x)g(x)]=g(x)$

上式说明，$p(x)\mid g(x)$。证完。

定理 8 F为域，$F[x]$中任一次数大于0的元$f(x)$都能表为F上有限个不可约多项式之积，而且不计次序和$\dot{F}$中的元的差别，这种表法是唯一的，即若

$$f(x)=p_1(x)p_2(x)\cdots p_r(x)=q_1(x)q_2(x)\cdots q_s(x)$$

则 $r=s$，而且适当调换次序，有

$$p_i(x)=c_iq_i(x),\ i=1,\ 2,\ \cdots,\ r,\ c_i(\neq 0)\in F$$

其中，$p_i(x)$ 和 $q_i(x)$ 都是F上的不可约多项式。

定理 8 的证明与数域上多项式环中的因式分解定理的证明完全类似，故从略。

习　　题

1　I是整环，在$I[x]$中证明，

（1）若$f_1(x)\mid f_2(x)$，$f_2(x)\mid f_3(x)$ 则 $f_1(x)\mid f_3(x)$；

（2）若$d(x)\mid f_1(x)$，$f_2(x)$，则 $d(x)\mid f_1(x)g_1(x)+f_2(x)g_2(x)$，其中，$g_1(x)$和$g_2(x)$是 $I[x]$中任意元；

（3）$f(x)$，$g(x)$ 不全为 0，$f(x)\mid g(x)$，$g(x)\mid f(x)$ 必要而且只要：$f(x)=cg(x)$，$g(x)=df(x)$，其中 c，d是I中的单位（可逆元）。

2　设I是整环，$f(x)\in I[x]$，c_1，c_2，…，c_r 是 $f(x)$的 r 个不同的根而且c_i是 $f(x)$的 k_i 重根（$i=1$，2，…，r）。证明：$(x-c_1)^{k_1}(x-c_2)^{k_2}\cdots(x-c_r)^{k_r}\mid f(x)$。

3　求 $\mathbf{Z}_7[x]$中的元：x^7-1 的所有根。

4　设F为域，证明$F[x]$中次数大于 0 的元都能表为F上的有限个

不可约多项式之积.

5　I是整环，$g(x)=bx+c\in I[x]$且b为I中的单位. 证明：$I[x]$中任意元$f(x)$被$g(x)$除所得的余式等于$f(-b^{-1}c)$.

6　证明本节定理2和导数规则.

7　$F_1=\boldsymbol{Z}_3$，$F_2=\boldsymbol{Z}_5$. 试判断x^2+1在$F_1[x]$和$F_2[x]$中是否是不可约多项式.

8　设F是域，$f(x)$，$g(x)\in F[x]$. 如果$F[x]$中的元$d(x)$满足条件：

（1）$d(x)|f(x)$，$g(x)$；

（2）$d(x)$能被$f(x)$与$g(x)$的任一公因子$d_0(x)$整除.

则$d(x)$叫做$f(x)$与$g(x)$的最大公因子. 证明本节定理6中的$d(x)$是$f(x)$与$g(x)$的最大公因子.

9　设F是域. 证明：$F[x]$中任二元$f(x)$和$g(x)$在$F[x]$中一定有最大公因子而且（不计单位因子）是唯一的，即$\overline{d}(x)$，$d(x)$都是$f(x)$和$g(x)$的最大公因子时，则$\overline{d}(x)=\varepsilon d(x)$，$\varepsilon$是$F[x]$中的单位.

10　设F是域，$p(x)$是$F[x]$中的不可约多项式. 证明：$(p(x))$是$F[x]$的极大理想.

注：习题中的x都是未定元.

§11　唯一分解环

上节最后，我们把整数环的唯一分解定理推广到域F上的多项式环. 从环的角度看，整数环$\boldsymbol{Z}$和域F上的一元多项式环$F[x]$都是整环. 本节将把所谓唯一分解定理推广，往证：对主理想环唯一分解定理成立.

为此目的，首先需要把整数环中的整除、素数两个概念推广到一般整环中去.

定义1　I是整环，a，$b\in I$. 如果在I中存在q，使

$$a=bq$$

成立，则说b整除a，记作：$b|a$. 这时b叫做a的因子，a叫做b的倍元. 若b不能整除a，则记作：$b\nmid a$.

令U是整环I中所有单位（可逆元）的集合，显然，U是

乘群（关于 I 的乘法）。

命题 1 设 a，b是 I 中不全为0的元，则 $a|b$，$b|a$，必要而且只要存在 $u\in U$，使$b=ua$。

证明 充必性。若$b=ua$，当然有$a|b$。另一方面，因$u\in U$，故有$u^{-1}\in U\subseteq I$，用 u^{-1}乘上式，得到

$$u^{-1}b=a$$

即 $b|a$。充分性得证。

必要性。若 $a|b$，$b|a$，则有 q_1，$q_2\in I$ 使得

$$b=aq_1,\quad a=bq_2$$

于是有

$$b=(bq_2)q_1=b(q_2q_1)$$

因为a，b不全为0，故由$a=bq_2$ 可知$b\neq 0$。则由$b=b(q_2q_1)$，根据在整环中消去律成立，得到

$$q_2q_1=1$$

即 q_1，$q_2\in U$。证完。

定义 2 a，$b\in I$，如果存在 $\varepsilon\in U$（即 ε 是 I 的单位）使得：$b=\varepsilon a$，则称 b 为 a 的相伴元。

命题 2 （1）a 是 a 的相伴元；（2）若 b 是 a 的相伴元，则 a 是 b 的相伴元；（3）若 b 是 a 的相伴元，c 是 b 的相伴元，则 c 是 a 的相伴元。其中 a，b，$c\in I$。

证明 在整环 I 中，$a=1a$，$1\in U$，即 a 是 a 的相伴元，（1）得证。

若 b 是 a 的相伴元，则有：$b=\varepsilon a$，$\varepsilon\in U$。

因 ε 是 I 中的单位，所以有：$a=\varepsilon^{-1}b$，$\varepsilon^{-1}\in U$，即 a 是 b 的相伴元，（2）得证。

当 b 是 a 的相伴元，c 是 b 的相伴元时，则有：$b=\varepsilon_1 a$ $c=\varepsilon_2 b$，ε_1，$\varepsilon_2\in U$。

而 $c=\varepsilon_2 b=\varepsilon_2(\varepsilon_1 a)=(\varepsilon_2\varepsilon_1)a$，$\varepsilon_2\varepsilon_1\in U$（因 U 是 I 中所有单位构成的乘群），所以 c 是 a 的相伴元，（3）得证。证完。

命题 2 说明：相伴关系是整环 I 上的一个等价关系。

由于在整环中，总有：$a=\varepsilon(\varepsilon^{-1}a)$，$\varepsilon\in U$，所以 I 中的任一单位和 a 的相伴元都整除 a，即 I 中的单位和 a 的相伴元都是 a 的因子。我们称它们为 a 的平凡因子。

如果整环 I 中的元 a 除了平凡因子之外，还有其它因子 b，则称 b 为 a 的真因子。

定义 3　I 中的元 p 如果既不是零元又不是单位，而且 p 只有平凡因子时，则称 p 为 I 的素元。

例 1　整数环 $\mathbf{Z}$ 中的素数都是 $\mathbf{Z}$ 的素元，由于 $\mathbf{Z}$ 中的单位只有 1 和 -1，所以 $a\in\mathbf{Z}$，a 的相伴元只有 $\pm a$。

例 2　域 F 上的多项式环 $F[x]$ 中的所有单位（可逆元）所构成的乘群为 $\dot{F}$，$F[x]$中的不可约多项式是 $F[x]$ 的素元（$\dot{F}$是$\{0\}$在 F 中的补集）。

关于相伴元和素元，有下面的性质

命题 3　（1）a 与其相伴元 εa 有相同的因子。即 a 的因子必是其相伴元εa的因子，εa 的因子也必是 a 的因子；

（2）整环 I 中的素元 p 的相伴元εp仍是 I 的素元。

证明　若$b|a$，显然 $b|\varepsilon a$，即 a 的因子必是其相伴元 εa 的因子。因为 a 是其相伴元 εa 的相伴元，所以由上证可知εa 的因子也必是 a 的因子。（1）得证。

由（1）显然可知，当 p 是整环 I 的素元时，则 p 的相伴元εp也必是 I 的素元，（2）得证。证完。

定义 4　如果对整环 I 中任意元 a（$a\neq0$）且 $a\bar{\in}U$，即 a 既不是 0 元也不是单位），都能写为 I 中有限个素元之积，而且，若

$$a=p_1p_2\cdots p_r=q_1q_2\cdots q_s，\text{其中 } p_i \text{ 和 } q_j \text{ 都是 } I \text{ 的素元}$$

则有：$r=s$，并且可适当调换 q_i 的次序，使得：$q_i=\varepsilon_ip_i$（ε_i是 I 的单位）则称整环 I 为唯一分解环。

例 3　整数环是唯一分解环，域 F 上的一元多项式环$F[x]$也是唯一分解环（由 §10定理 8）。

例4　令 $I=\{a+b\sqrt{-3} \mid a, b$ 为任意整数$\}$，则 I 不是唯一分解环。

解　显然 I 是整环，应用复数的模的性质可知

（1）I 的元 ε 是单位必要而且只要 $|\varepsilon|^2=1$，从而 I 只有两个单位，就是 ± 1。

事实上，若 $\varepsilon=a+b\sqrt{-3}$ 是 I 的单位，则有 $\varepsilon'=a'+b'\sqrt{-3}$ 使得：$\varepsilon\varepsilon'=1$。

因为 $|1|^2=|\varepsilon|^2|\varepsilon'|^2$，而 $|1|^2=1$，所以

$$|\varepsilon|^2|\varepsilon'|^2=1$$

但是 $|\varepsilon|=\sqrt{a^2+(b\sqrt{3})^2}$，$|\varepsilon|^2=a^2+3b^2$，

所以 $|\varepsilon|^2$ 是一个正整数（因 a，b 不能同时为0），同理，$|\varepsilon'|^2$ 也是一个正整数。从而得到：$|\varepsilon|^2=1$。

反之，若 $\varepsilon=a+b\sqrt{-3}$，$|\varepsilon|^2=1$。于是由模的定义有：$a^2+3b^2=1$。

因为 a，b 都是整数，所以必有 $a=\pm 1, b=0$，即 $\varepsilon=\pm 1$。而 ± 1 是 I 的单位是显然的。

综上所述，可知 ε 是 I 的单位必要而且只要 $|\varepsilon|^2=1$，而且 ± 1 是 I 的仅有的两个单位。

（2）$\alpha\in I$，若 $|\alpha|^2=4$，则 α 是 I 的素元。

首先，由 $|\alpha|^2=4$，可知 $\alpha\neq 0$，而且由（1）可知 α 不是 I 的单位。

如果设 $\beta=a+b\sqrt{-3}$ 是 α 的因子，则有 $\alpha=\beta\gamma$。

则　$|\alpha|^2=|\beta|^2|\gamma|^2=4$

由于 $|\beta|^2=a^2+3b^2$ 和 $|\gamma|^2$ 都是正整数，所以由 $|\beta|^2\cdot|\gamma|^2=4$ 可知 $|\beta|^2$ 只能是 4 的正因数。而 4 的所有正因数为 1，2，4。但是，不论 a，b 取任何整数，$|\gamma|^2=a+3b^2\neq 2$，所以 $|\beta|^2=1$ 或 4。

如果 $|\beta|^2=1$，则由（1）知 β 是单位；

如果 $|\beta|^2=4$，则由 $|\beta|^2|\gamma|^2=4$ 有 $|\gamma|^2=1$。从而 γ 是单位，所以 $\beta=\gamma^{-1}\alpha$。上式说明 β 是 α 的相伴元。

综合上述可知，当 $|\alpha|^2=4$ 时，α 是 I 的素元。

对于 I 中的元 4 来说，显然有

$$4=2\cdot 2=(1+\sqrt{-3})(1-\sqrt{-3})$$

因为，$2=2+0i$，$|2|^2=(\sqrt{2^2+0^2})^2=4$

$$1+\sqrt{-3}=1+\sqrt{3}\,i,$$

$$|1+\sqrt{-3}|^2=(\sqrt{1+(\sqrt{3})^2})^2=4$$

$$1-\sqrt{-3}=1-\sqrt{3}\,i,$$

$$|1-\sqrt{-3}|^2=(\sqrt{1+(-\sqrt{3})^2})^2=4$$

所以由（2）知，2，$1+\sqrt{-3}$，$1-\sqrt{-3}$都是 I 的素元。而且，$1+\sqrt{-3}$和$1-\sqrt{-3}$都不是 2 的相伴元。

因此，I 中的元 4 分解为素元之积的形式不是唯一的，所以 I 不是唯一分解环。

由上例看出，整环不都是唯一分解环，那么，哪样一些整环是唯一分解环？一般来说想确定一个整环是唯一分解环是比较困难的。但是，可以证明主理想整环一定是唯一分解环。

定理 1　主理想环 I 中的非单位 $p(\neq 0)$ 是素元必要而且只要（p）是素理想。

证明　先证充分性。设$p(\neq 0)$是 I 中的非单位，而且(p)是 I 的素理想，往证 p 是 I 的素元。为此只须证明 p 只有平凡因子即可。

设　$p=ab$，则 $p=ab\in(p)$。

由素理想定义有 $a\in(p)$或$b\in(p)$。

若$a\in(p)$时，则有 $q\in I$ 使$a=pq$。将它代入 $p=ab$ 得到

$$p=(pq)b=p(qb)$$

于是由$p\neq 0$和消去律得到

$$qb=1$$

上式说明，q 和 b 都是 I 中的单位。

若$b\in(p)$时，则有$q'\in I$使$b=pq'$。把它代入$p=ab$ 得到

$$p=a(pq')=p(aq')$$

于是由$p\neq 0$和消去律得到

$$aq' = 1$$

上式说明，a 和q'都是 I 中的单位。

综合上述可知，非单位$p(\neq 0)$只有平凡因子，即 p 是 I 的素元。

其次证明必要性。

若 p 是 I 的素元，往证(p)是 I 的素理想。若$(p) = I$，显然 (p)是 I 的素理想。若 $(p) \neq I$，因为 I 是有 1 的交换环，所以只要能证得(p)是 I 的极大理想，则由 § 7 推论 1 即得(p)是素理想。

设 J 是 I 的理想且$J \supset (p)$，则由题设 I 是主理想环，故有$J = (d)$。因为 $p \in (p) \subset J = (d)$，所以 $p = dq$。因为 p 为 I 的素元，所以$d = \varepsilon$，或$d = \varepsilon p$。其中，ε 是 I 的单位。若$d = \varepsilon p$，则 $p = \varepsilon^{-1}d$。因此有 $(d) = (p)$，这与 $J = (d) \supset (p)$ 相矛盾，所以$d = \varepsilon$。于是进一步由 J 是理想，可知 $\varepsilon\varepsilon^{-1} = 1 \in J = (\varepsilon)$。而$x = 1 \cdot x$，$x \in I$。故有 $J = (\varepsilon) = I$。

于是证得 (p) 是 I 的极大理想，从而由 § 7 推论 1，可知(p)是 I 的素理想。证完。

推论 1　若 p 是主理想环的素元，如果$p|ab$则$p|a$或$p|b$。

事实上，由定理 1 知，当 p 是素元时，(p) 是素理想。所以若 $p|ab$，则有 $ab \in (p)$。于是，由素理想的定义，则有 $a \in (p)$，或$b \in (p)$。从而有$a = pq_1$，或$b = pq_2$。即$p|a$或$p|b$。

定理 2　主理想环 I 是唯一分解环。

证明　若

$$a = p_1p_2\cdots p_s = q_1q_2\cdots q_t \qquad (*)$$

其中，p_i和 q_j都是 I 的素元。往证：$s = t$，而且适当调换次序有：$q_i = \varepsilon_i p_i$，$i = 1, 2, \cdots, s$，其中 ε_i是 I 中的单位。

$(*)$ 式说明：$q_1 | p_1p_2\cdots p_s$，而q_1是主理想环 I 的素元，故由定理 1 推论可知q_1必整除某一p_i，适当调换 p_i的次序，则可设$q_1 | p_1$。即q_1为素元p_1的因子。但q_1也是素元，所以 q_1 不能是单位。而素元p_1只有平凡因子，所以q_1是p_1的相伴元，即q_1

$=\varepsilon_1 p_1$，其中，ε_1 为 I 的单位。

将$q_1=\varepsilon_1 p_1$ 代入（*）式然后消去 p_1，得到

$$p_2\cdots p_s=q_2\cdots q_t$$

如此继续下去，即可推得 $s=t$，而且

$$q_i=\varepsilon_i p_i,\quad i=1,\ 2,\ \cdots,\ s$$

下面来证明 I 中不是单位的元素$a(\neq 0)$都可分解为 I 的有限个素元之积。我们用反证法。假定 a 不能分解为有限个素元之积。显然，a 不能是素元，故有 $a=bc$，其中 b 和 c 都是 a 的真因子。这时，自然 b 与 c 至少有一个不能分解为有限个素元之积，设它为a_1。这时 $a_1|a$，a_1 既不是 a 的相伴元而且也不是素元，进一步可以推得a_1也一定存在一个非平凡因子 a_2，而且a_2也不能分解为有限个素元之积。继续下去，可以得到：由 I 的不能分解为有限个素元之积的元所构成的无穷序列

$$a_1,\ a_2,\ \cdots$$

其中，$a_{i+1}|a_i$，a_{i+1}不是a_i 的相伴元（即 $a_i\nmid a_{i+1}$）。现在来考虑 I 的主理想

$$(a_1),\ (a_2),\ (a_3),\cdots$$

由于 $a_{i+1}|a_i$，所以有

$$(a_1)\subseteq(a_2)\subseteq(a_3)\subseteq\cdots$$

令 U_0 是这些主理想的并集，显然U_0 是 I 的理想。但由题设 I 是主理想环，所以存在$d\in I$使得 $U_0=(d)$。因为 U_0 是所有 (a_j) 的并集，所以$U_0\supseteq$每一(a_j)，$j=1,\ 2,\ \cdots$，从而有 $d|a_j$，$j=1,2,\cdots$。另一方面，因为 I 是整环有 1，所以 $d\cdot 1=d\in U_0$，而 U_0 是所有(a_j)的并集，则 d 属于某一(a_n)。所以 $a_n|d$。

上面已证得 $d|$每一$a_j(j=1,2,\ \cdots)$，当然$d|a_{n+1}$则由 $a_n|d$得到：$a_n|a_{n+1}$与$a_n\nmid a_{n+1}$ 矛盾。综上所述，可知 I 中任意不是单位的非零元 a 都能分解为 I 中的有限个素元之积，证完。

我们已经知道，整数环Z和域 F 上的多项式环 $F[x]$都是主理想环，所以作为定理 2 的直接结果，可知它们都是唯一分解

环。

在证明整数环和域F上的一元多项式环都是主理想环时，我们看到关键在于两个环都可以作带余除法。一般来说，我们引进

定义 5 设R是整环，如果R中每个非零元b都能对应唯一一个非负整数$\delta(b)$，使得R中任一元a都能表为

$$a=bq+r,\ q,\ r\in R$$

其中，$r=0$或$\delta(r)<\delta(b)$，则称整环R为欧氏环。

例 5 整数环$\mathbf{Z}$和域F上的多项式环$F[x]$都是欧氏环。

解 对$\mathbf{Z}$规定：$\delta(a)=|a|$，$a(\neq 0)\in\mathbf{Z}$。

对$F[x]$规定：$\delta(f(x))=\deg f(x)$，$f(x)(\neq 0)\in F[x]$。则由在$\mathbf{Z}$和$F[x]$中带余除法定理成立，所以$\mathbf{Z}$和$F[x]$都是欧氏环。

由例 5 容易看出，域$F\subseteq F[x]$，故域F一定是欧氏环。

定理 3 欧氏环一定是主理想环。

证明作为练习。

于是由定理 2 可知，欧氏环也是唯一分解环。

最后再给出唯一分解环的一个重要性质。

定义 6 I是唯一分解环，$c\in I$。如果$c\mid a_1, a_2, \cdots, a_n$ $(a_i\in I)$时，则称c为$a_1, a_2, \cdots, a_n$的公因子。若d是$a_1, a_2, \cdots, a_n$的公因子，而且d能被$a_1, a_2, \cdots, a_n$的任一公因子c整除，则称d为$a_1, a_2, \cdots, a_n$的最大公因子。

定理 4 唯一分解环I中的两个元a和b一定有最大公因子，而且a和b的两个最大公因子d和$\bar{d}$互为相伴元：$\bar{d}=\varepsilon d$，ε是I的单位。

证明 若a和b中有一个是零，例如$b=0$，则a与b的最大公因子为a；若a与b中有一个是单位，例如，$b=\varepsilon$（单位），则a与b的最大公因子是b。

下面考虑a和b都不是零而且也不是单位的情形。则由I是唯一分解环，所以有

$$a = p_1p_2\cdots p_r,\quad b = p'_1p'_2\cdots p'_s$$

其中p_i和p'_i都是素元。

p_i和p'_i这$r+s$个素元中，某一个可能是其它一个的相伴元。这时，我们假定在这$r+s$个元中有n个元，互相不是相伴元，设为$p_1, p_2, \cdots, p_n$。则可将a和b写为下面的形式：

$$a = \varepsilon_a p_1^{k_1} p_2^{k_2}\cdots p_n^{k_n}\ (\varepsilon_a \text{ 是 } I \text{ 的单位}, k_i \geqslant 0)$$

$$b = \varepsilon_b p_1^{h_1} p_2^{h_2}\cdots p_n^{h_n}\ (\varepsilon_b \text{ 是 } I \text{ 的单位}, h_i \geqslant 0)$$

令$l_i = \min(k_i, h_i)$，则$d = p_1^{l_1} p_2^{l_2}\cdots p_n^{l_n}$是$a$与$b$的最大公因子。事实上，显然有$d\mid a$，$d\mid b$，即$d$是$a$与$b$的公因子。其次。若$c\mid a, b$。如果$c$是单位，当然$c\mid d$。如果$c$不是单位，当然不是零元，于是在$I$中有分解：$c = q_1q_2\cdots q_t$（$q_i$是素元）。由于$c\mid a$，$q_i$是素元，所以必有$q_i\mid$某一$p_j$，从而$q_i$是$p_j$的相伴元。所以有

$$c = \varepsilon_c p_1^{m_1} p_2^{m_2}\cdots p_n^{m_n}\ (\varepsilon_c \text{是} I \text{ 的单位}, m_i \geqslant 0)$$

因为$c\mid a$，而且p_i和p_j互相不是相伴元，所以$m_i \leqslant k_i$。同理，由$c\mid b$，可得$m_i \leqslant h_i$。从而有$m_i \leqslant l_i$，$c\mid d$。这样就证明了d是a与b的最大公因子。综合上述，可知I中任意两个元a与b一定有最大公因子存在。

最后证明a与b的任意两个最大公因子d和$\overline{d}$互为相伴元。当d和$\overline{d}$都是a与b的最大公因子时，则有$d\mid\overline{d}$，$\overline{d}\mid d$，于是有：$\overline{d} = dq_1$，$d = \overline{d}q_2$，从而有$\overline{d} = \overline{d}q_2q_1$。

若$\overline{d} = 0$，则$d = \overline{d}q_2 = 0q_2 = 0$，即$d = \overline{d}$。若$\overline{d} \neq 0$，由$\overline{d} = \overline{d}q_2q_1$消去$\overline{d}$得到

$$q_2q_1 = 1$$

即q_1和q_2是单位，即$\overline{d} = \varepsilon d$或$d = \varepsilon\overline{d}$。证完。

应用定理 4 作归纳法可得到

推论 2　唯一分解环I中的n个元：$a_1, a_2, \cdots, a_n$在I里一定有最大公因子，而且它们的任意两个最大公因子互为相伴元。

定义 7　I是唯一分解环，如果$a_1, a_2, \cdots, a_n$的最大公因

子是单位，则称 $a_1, a_2, \cdots, a_n$ 互素，记作：$(a_1, a_2, \cdots, a_n) = 1$。

显然，对唯一分解环所定义的最大公因子和互素的概念是普通最大公因子和互素概念的推广。

习　　题

1　指出在 $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$ 中，5 是素元但 7 不是素元。

2　证明：$\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$ 是欧氏环，并指出 3 是素元但 5 不是素元，再进一步把 5 表为素元之积。

3　指出 $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbf{Z}\}$ 不是唯一分解环。

4　证明：欧氏环是主理想环。

5　证明：域是欧氏环。

6　I 为主理想环，$a, b \in I$，d 为 a 与 b 的最大公因子。证明：在 I 中存在 u, v 使得

$$au + bv = d$$

7　$S_p = \{\frac{a}{b} \in \mathbf{Q} \mid a, b \in \mathbf{Z}, p \nmid b\}$（$p$ 是素数）。证明：S_p 是唯一分解环。

8　I 是唯一分解环，$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in I[x]$。如果 $(a_n, a_{n-1}, \cdots, a_1, a_0) = 1$，则称 $f(x)$ 为本原多项式。证明：$I[x]$ 中任二本原多项式之积仍是本原多项式。

第四章　模

模是数域上线性空间的推广．它在研究抽象环到交换群的自同态环内同态时，是非常重要的．本章侧重于介绍环上的线性代数知识，对一般模论的内容不做深入的探讨．

§1　模的定义

先回顾一下"高等代数"中线性空间的定义．

设 F 是数域，$\{V;\ +\}$是加群，如果规定 F 乘 V 到 V 的运算"·"满足

（1）$a\cdot(x+y)=a\cdot x+a\cdot y$

（2）$(a+b)\cdot x=a\cdot x+b\cdot x$

（3）$(ab)\cdot x=a\cdot(b\cdot)x$

（4）$1\cdot x=x$

$\forall a,b\in F,\ x,\ y\in V$．则称 V 为数域 F 上的线性空间，运算"·"称为 F 乘 V 到 V 的作用乘法．

数域 F 上的线性空间 V，是由数域 F 和加群 V 在作用乘法下所成的代数体系．如果将数域 F 放宽成一般的环 R，就得到了一个推广的代数体系——模．

定义1　设 R 是环，M 是加群，如果规定 R 乘 M 到 M 的代数运算"·"满足

（1）$a\cdot(x+y)=a\cdot x+a\cdot y$

（2）$(a+b)\cdot x=a\cdot x+b\cdot x$

（3）$(ab)\cdot x=a\cdot(b\cdot x)$　　$\forall a,b\in R,\ x,y\in M$．

则称 M 为环 R 上的左模，简记为 R—左模 M．称代数运算

“·”为R乘M的左倍乘运算。以后常将 $a\cdot x$ 略记为 ax。

在R—左模M中，称R的元素为标量，称M中元素为模元素。为了清楚，常将标量的零元记为 0 ，将模元素的零元记为 θ ，由模的定义，可直接推得

（1） $a\theta = 0x = \theta$

（2） $(-a)x = a(-x) = -(ax) \quad \forall\ a\in R, x\in M$

事实上因为

$$a\theta = a(\theta+\theta) = a\theta + a\theta$$

由M是加群，可得 $a\theta=\theta$。又因为

$$0x = (0+0)x = 0x + 0x$$

同理亦得 $0x=\theta$，故（1）成立。再由

$$ax + (-a)x = [a+(-a)]x = 0x = \theta$$

及M是加群，可得 $-(ax) = (-a)x$；同样，由

$$ax + a(-x) = a[x+(-x)] = a\theta = \theta$$

知：$-(ax) = a(-x)$。故（2）也成立。

例 1 设R是环，M是加群。$\forall a\in R$，$x\in M$ 如果规定：$a\cdot x=\theta$。则加群M与环R，在代数运算“·”下构成R—左模，称此模为零模。

例 2 设$\{R;+,\times\}$是环，则$\{R;+\}$是加群。$\forall a,x\in R$，如果规定

$$a\cdot x = a\times x$$

则在运算“·”下，加群$\{R;+\}$构成环$\{R;+,\times\}$上的左模，称为环模。

例 3 设R是偶数环，$M=R\oplus R$，是由偶数加群做成的（外）直和。$\forall a\in R$，$(x,y)\in M$，如果规定

$$a\cdot(x,y) = (ax,ay)$$

则在运算“·”下，M构成R上的左模。

在数域F上的线性空间V中，由于

（4） $1\cdot x = x,\quad \forall x\in V$

可知

$$FV=\left\{\sum_{i=1}^{n} a_i x_i \mid \forall a_i\in F,\ x_i\in V;\ \forall n\in N\right\}=V$$

但在环R上的左模M中，

$$RM=\left\{\sum_{i=1}^{n} a_i x_i \mid \forall a_i\in R, x_i\in M;\ \forall n\in N\right\}=M$$

却不一定再成立了。通过例1，不难举出这方面的实例。在例3中，也具有$RM\neq M$这一特性，于是我们给出

定义2　对于R—左模M。如果满足

$$RM=M$$

则称M为R上的左单式模。

定理　设R是有$1\neq 0$的环，那么R上的左模M是单式的，必要而且只要

（4）$1x=x,\quad \forall x\in M$

成立。

证明　若（4）$1x=x$，$\forall x\in M$成立。则$\forall x\in M$，都有$x=1x\in RM$，故$M=RM$。于是知M是R上左单式模。

若M是R上左单式的。由$M=RM$知$\forall x\in M$，x总可表为

$$x=\sum_{i=1}^{n} a_i x_i,\quad a_i\in R,\ x_i\in M,\ i=1,2,\cdots,n$$

于是

$$1x=\sum_{i=1}^{n}(1a_i)x_i=\sum_{i=1}^{n} a_i x_i=x$$

故（4）成立。证完。

这里要注意，构成单式模的环不一定有1。

例4　设R为偶数环，M为有理数加群，在数的倍乘运算下，M是R上的左模。此时R没有1，但是$RM=M$，是单式模。

从定义可知，有1的环上的单式模是较近于线性空间的一种模。

设R是有$1\neq 0$的环，M是R上的左模，$\forall x\in M$，都有$x=(x-1x)+1x$，于是加群M可分解为子群

$$M_0=\{x_0\in M\mid x_0=x-1x,\quad \forall x\in M\}$$

和子群

$$M_1=\{x_1\in M\mid x_1=1x,\forall x\in M\}$$

的（内）直和，即

$$M=M_0\oplus M_1$$

其中M_0构成R上的零模，M_1构成R上的单式模，而零模的结构是清楚的，因此重点研究有$1\neq 0$环上单式模就可以了。

类似于左模，可以定义右模。

设　R是环，M是加群，如果规定M乘R到M的代数运算"·"满足

(1′) $(x+y)\cdot a=x\cdot a+y\cdot a$

(2′) $x\cdot(a+b)=x\cdot a+x\cdot b$

(3′) $x\cdot(ab)=(x\cdot a)\cdot b\quad \forall\ x,y\in M,\ a,b\in R,$

则称M为环R上的右模。代数运算"·"称为右倍乘运算。

仿左模的有关定义，可给出右单式模、右零模，……等概念。

例5　设$\mathbf{Z}$是整数加群

$$\mathbf{Z}^{(n+1)}=\mathbf{Z}\oplus\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}$$

$$M_n(\mathbf{Z})=\left\{\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\vdots\\ a_{n1}&\cdots&a_{nn}\end{pmatrix}\middle|\ a_{ij}\in\mathbf{Z}\quad {}_{1\leqslant i,j\leqslant n}\right\}$$

是整数环$\mathbf{Z}$上的n阶矩阵环。$\forall\ x=(x_1\ x_2\cdots\ x_{n+1})\in\mathbf{Z}^{(n+1)}$，$A=(a_{ij})\in M_n(\mathbf{Z})$，规定右倍乘"·"为

$$x\cdot A=((x_1x_2\cdots x_n)A,\ 0)$$

则$\mathbf{Z}^{(n+1)}$是$M_n(\mathbf{Z})$上的右模，加群$\mathbf{Z}^{(n+1)}$可分解为

$$\mathbf{Z}^{(n+1)}=M_0\oplus M_1$$

其中子群

$$M_0=\{(0,\cdots,0,x_{n+1})\in\mathbf{Z}^{n+1}\mid x_{n+1}\in\mathbf{Z}\}$$

$$M_1=\{(x_1,\cdots,x_n,0)\in\mathbf{Z}^{(n+1)}\mid x_i\in\mathbf{Z}_{,i=1,2,\cdots,n}\}$$

是环$M_n(\mathbf{Z})$上的右零模和右单式模。

做为左模和右模的差别，初看起来容易认为是倍乘之积的记法问题．而实质上是运算条件(3)和(3′)所表现出来的标量因子对模元素倍乘时的顺序问题．在R—左模M中，有

(3) $(ab)x=a(bx)\quad \forall a,b\in R,\ x\in M$．标量之积$ab$左倍乘模元素$x$，分解成标量因子$a$，$b$逐次倍乘$x$〔即$a(bx)$〕时，先从标量之积$ab$的右因子$b$开始，逐次向左进行；而在$R$—右模$M$中，有

(3′) $x(ab)=(xa)b\quad \forall x\in M,a,b\in R$．标量之积$ab$右倍乘模元素$x$，分解成标量因子$a$，$b$逐次倍乘$x$〔即$(xa)b$〕时，先从标量之积$ab$的左因子$a$开始，逐次向右进行．

从这一差别中可看到左模和右模的联系，可以将左模的理论平行的移到右模上，所以我们只须重点研究左模就够了．以后将研究重点放在左单式模上．

例 6 设$\mathbf{Z}$是整数环

$$\mathbf{Z}^{(n)}=\mathbf{Z}\oplus\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}$$

$\forall\ x=(a_1,a_2,\cdots,a_n)\in\mathbf{Z}^{(n)}$，$a\in\mathbf{Z}$，令

$$a\cdot x=(aa_1,aa_2,\cdots,aa_n)$$

则$\mathbf{Z}^{(n)}$在倍乘运算“·”下，构成$\mathbf{Z}$上的左单式模．

例 7 设$\mathbf{Z}$是整数环

$$\mathbf{Z}^{(n)}=\mathbf{Z}\oplus\mathbf{Z}\oplus\cdots\oplus\mathbf{Z}$$

$$M_n(\mathbf{Z})=\left\{\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\vdots\\ a_{n1}&\cdots&a_{nn}\end{pmatrix}\middle|\ a_{ij}\in\mathbf{Z},1\leqslant i,\ j\leqslant n\right\}$$

$\forall\ x=(a_1,a_2,\cdots,a_n)\in\mathbf{Z}^{(n)}$，$A=(a_{ij})\in M_n(\mathbf{Z})$，令

$$x\cdot A=(a_1\ a_2\cdots a_n)A$$

则$\mathbf{Z}^{(n)}$在倍乘运算“·”下，做成环$M_n(\mathbf{Z})$上的右单式模．

例 8 在例6中，令

$$x\circ a=a\cdot x$$

则$\mathbf{Z}^{(n)}$关于运算“∘”，构成$\mathbf{Z}$上的右单式模．

解 显然“∘”是$\mathbf{Z}^{(n)}$乘$\mathbf{Z}$到$\mathbf{Z}^{(n)}$的代数运算，且满足

(1′) $(x+y)\circ a=a\cdot(x+y)=a\cdot x+a\cdot y$

$$=x\circ a+y\circ a$$

(2′) $x\circ(a+b)=(a+b)\cdot x=a\cdot x+b\cdot x$

$$=x\circ a+x\circ b$$

(3′) $x\circ(ab)=(ab)\cdot x=(ba)\cdot x=b\cdot(a\cdot x)$

$$=b\cdot(x\circ a)=(x\circ a)\circ b$$

(4′) $x\circ 1=1\cdot x=x$

$\forall\ x,y\in Z^{(n)},a,b\in Z$，都成立。于是知 $Z^{(n)}$关于代数运算“∘”做成Z上的右单式模。

例9　在例7中，令

$$A\circ x=x\cdot A\quad \forall A\in M_n(Z),\ x\in Z^{(n)}$$

那么$Z^{(n)}$关于运算“∘”是否是$M_n(Z)$上的左模呢？

解　不是。因为$\forall\ A,\ B\in M_n(Z)$，$x\in Z^{(n)}$，据“∘”的定义有

$$(AB)\circ x=x(AB)$$

$$A\circ(B\circ x)=A\circ(xB)=(xB)A=x(BA)$$

由于$Z_n(M)$是非可换环，故存在$A_1,B_1\in M_n(Z)$ 使

$$(c_{ij})=A_1B_1\neq B_1A_1=(d_{ij})$$

于是存在　$1\leqslant i_1,j_1\leqslant n$，使　$c_{i_1j_1}\neq d_{i_1j_1}$。从而有

$x_1=(\underbrace{0\cdots0\ 1}_{i_1}\ 0\cdots0)\in Z^{(n)}$使

$$x_1(A_1B_1)=(c_{i_11}\,c_{i_12}\cdots c_{i_1j_1}\cdots c_{i_1n})$$

$$x_1(B_1A_1)=(d_{i_11}\,d_{i_12}\cdots d_{i_1j_1}\cdots d_{i_1n})$$

故知

$$x_1(A_1B_1)\neq x_1(B_1A_1)$$

$$(A_1B_1)\circ x_1\neq A_1\circ(B_1\circ x_1)$$

于是断定：关于运算“∘”，$Z^{(n)}$不是$M_n(Z)$上的左模。

例10　在例7中，令

$$x\cdot A=xA',\quad \forall\ A\in M_n(Z),\ x\in Z^{(n)}$$

则$Z^{(n)}$关于运算“∘”构成环$M_n(Z)$上的左单式模。

解 显然"$\circ$"是$M_n(Z)$乘$Z^{(n)}$到$Z^{(n)}$的代数运算，且有

（1）$A\circ(x+y)=(x+y)A'=xA'+yA'$
$$=A\circ x+A\circ y$$

（2）$(A+B)\circ x=x(A+B)'=x(A'+B')$
$$=xA'+xB'=A\circ x+B\circ x$$

（3）$(AB)\circ x=x(AB)'=x(B'A')=(xB')A'$
$$=(B\circ x)A'=A\circ(B\circ x)$$

（4）$E\circ x=xE'=xE=x$

$\forall\ x,y\in M$，$A,B\in M_n(Z)$ 都成立，其中E是$M_n(Z)$中单位阵，是环$M_n(Z)$中的1。于是断言：$Z^{(n)}$关于代数运算"$\circ$"构成环$M_n(Z)$上的左单式模。

例11　Z是整数环，M是加群，据群的运算定义有：$\forall\ a\in M$，$n\in Z$

$$na=\begin{cases}\underbrace{a+a+\cdots+a}_{n\text{个}}, & n>0\\ \underbrace{(-a)+(-a)+\cdots+(-a)}_{n\text{个}}, & n<0\\ 0, & n=0\end{cases}$$

依此，自然给出Z乘M到M的左倍乘运算，M构成Z上的左模。称为Z—模。

例12　Z是整数环，$N=(2)$是Z中2所生成的理想。对于

$$N^{(2)}=N\oplus N$$

$\forall\ x=(x_1,x_2)\in N^{(2)}$，$a\in Z$，如果规定

$$ax=(ax_1,ax_2)$$

则关于此规定，$N^{(2)}$构成Z上的模。

对于任一环R，今后常用

$$R^{(n)}=\overbrace{R\oplus R\oplus\cdots\oplus R}^{n\text{个}}$$

表示R的加法群所作的（外）直和。

例12的更一般情况是，设R是环，A是R的左理想．则$A^{(+)}$一定是R上的左模．特别是环R的任一理想A，加法群$\{A;\ +\}$都可视为环R上的模．如对环Z_6来说

$N_1=\{\bar{0},\ \bar{2},\ \bar{4}\}$，$N_2=\{\bar{0},\ \bar{3}\}$

都是Z_6的理想．N_1，N_2关于加法所作成的群，关于Z_6的乘法，都做成Z_6上的模．

例13　Z是整数环，Z_6是以6为模的剩余类加群．$\forall k\in Z$，$\bar{a}\in Z_6$，如果规定

$$k\bar{a}=\overline{ka}$$

作为Z乘Z_6到Z_6的左倍乘运算，则Z_6构成Z上的左模．

习　　题

1　举出两个非零的，非单式模的例子，并将模的加群分解成两个子群的直和，使其一为环上的零模，其一为环上的单式模．

2　设M是交换环R上的左模，$\forall\ a\in R, x\in M$，如果规定

$x\cdot a=ax$

则M关于运算"·"成为R上的右模．

3　设M是非交换除环R上的左单式模；$\forall\ a\in R$，$x\in M$，如果规定

$x\cdot a=ax$

证明：M关于运算"·"，不做成R上的右模．

4　设M是非交换环R上的左模，φ是环R上的反自同构，即φ是R上的双射，且满足

（1）$\varphi(a+b)=\varphi(a)+\varphi(b)$

（2）$\varphi(ab)=\varphi(b)\varphi(a), \forall a,b\in R, \forall x\in M$，如果规定

$x\cdot a=\varphi(a)x$

则M关于运算"·"构成R上的右模

5　设M是环R上的左模，φ是环S到环R的满同态．如果规定

$a\cdot x=\varphi(a)x$，$\forall\ a\in S$，$x\in M$

则M关于"·"构成S上的左模。

6　设M是加群，证明：只有一种方法使M做成Z—模．

7　设Q是有理数域，M是Q上关于倍乘运算"·"所成的单式模．证明：M在Q上成模的倍乘运算只能是唯一的"·"．

8　设M是非零的有限加群，试问：M能成为有理数域$\mathbf{Q}$上的单式模吗？

§2　模的生成集

以下讨论的模，总指的是环R上的左单式模。对于R—模M，由于

$$M=RM=\left\{\sum_{i=1}^{n}a_ix_i \mid \forall a_i\in R, x_i\in M, n\in N\right\}$$

可知：若 $x\in M$，则有有限个模元素$x_1, x_2, \cdots, x_s\in M$使

$$x=\sum_{i=1}^{s}a_ix_i, a_i\in R, \quad i=1, 2, \cdots, s$$

对于$y\in M$，同样也有有限个元素$y_1, y_2, \cdots, y_t\in M$使

$$y=\sum_{j=1}^{t}b_jy_j \quad b_j\in R, \quad j=1, 2, \cdots, t$$

一般说来，M的子集$X=\{x_1, x_2, \cdots, x_s\}$和$Y=\{y_1, y_2, \cdots, y_t\}$是不相同的。因此促使我们考虑：是否存在$M$的子集$S$，$\forall z\in M$都能在$S$中找到有限个元素$z_1, z_2, \cdots, z_n$，将$z$表成

$$z=\sum_{k=1}^{n}c_kz_k, \quad c_k\in R, \quad k=1, 2, \cdots, n$$

这样的子集S如果存在，我们就可以通过S去研究R—模M，于是给出

定义1　**设S是R—模M的非空子集，如果$\forall x\in M$，都存在有限个元素$u_1, u_2, \cdots, u_r\in S$使**

$$x=\sum_{i=1}^{r}a_iu_i, \quad a_i\in R, \quad i=1, 2, \cdots, r$$

则称S是R—模M的生成集，记作$M=L(S)$。

类似的也可以定义右模的生成集。

如果R—模存在着有限个元素构成的生成集，则称R—模M为有限生成模；如果R—模M是由一个元素生成的，则称

R—模M为循环模。这时

$$M=L(x)=Rx=\{rx \mid \forall r\in R\}$$

R—模M一定存在生成集，模元素集M就是明显的一个。一般说来，生成集并不唯一。

下面考查一下§1中各例的生成集。

例1　对Z模$Z^{(n)}$来说，子集

$$S=\{e_i\in Z^{(n)} \mid e_i=(\overbrace{0\cdots0\,1}^{i}\,0\cdots0),i=1,2,\cdots n\}$$

就是Z—模$Z^{(n)}$的一个生成集。

事实上，$\forall x=(a_1,a_2,\cdots,a_n)\in Z^{(n)}$，都有

$$(a_1,a_2,\cdots,a_n)=a_1e_1+a_2e_2+\cdots+a_ne_n$$

例2　对于$M_n(Z)$—右模$Z^{(n)}$来说，模元素

$$e_1=(1,0,\cdots,0)$$

就是一个生成集。

事实上，$\forall x=(a_1,a_2,\cdots,a_n)\in Z^{(n)}$，则存在

$$A=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}\in M_n(Z)$$

使 $x=e_1A$，所以$Z^{(n)}$是$M_n(Z)$上的右循环模。

例3　对于Z—模$(2)^{(n)}$来说，子集

$$S=\{f_i\in(2)^{(n)} \mid f_i=(\overbrace{0,\cdots,0,2}^{i},0,\cdots,0),i=1,2,\cdots,$$

$n\}$是模$(2)^{(n)}$一个生成集。

事实上，$\forall\ (a_1,a_2,\cdots a_n)\in(2)^{(n)}$，则 $a_i\in(2)$，于是$a_i=k_i2,k_i\in Z$。因之有

$$\begin{aligned}(a_1,a_2,\cdots,a_n)&=(k_12,k_22,\cdots,k_n2)\\&=k_1f_1+k_2f_2+\cdots+k_nf_n\end{aligned}$$

于是知S是$(2)^{(n)}$的一个生成集。

例4　对于Z—模Z_6来说，子集

$$H=\{\overline{2},\ \overline{3}\}$$

就是一个生成集．

事实上，$\forall \overline{m}\in Z_6$，有

$$\overline{m}=\overline{m\times 1}=m\overline{1}$$
$$=m(\overline{3}-\overline{2})=m\overline{3}+(-m)\overline{2}$$

于是知 H 是 Z_6 在 Z 上的生成集．

显然 $\overline{1}$ 也是 Z_6 在 Z 上的生成集，故 Z_6 在 Z 上是循环模．

在以上各例中，生成集所含元素的个数都是有限的，它们都是有限生成模．下面再看一下无限生成模的例子．

例 5　设 R 是有 $1\neq 0$ 的交换环，x 是 R 上的未定元，那么多项式加群 $\{R[x];\ +\}$ 在 R 上是无限生成模．

事实上，对 $R[x]$ 的任一个有限子集 $S\neq\{0\}$ 来说，其中次数最高的多项式的次数是固定的非负整数 n．所以 S 中任意有限个元素 $f_1(x),\ f_2(x),\cdots,\ f_r(x)$ 所表出的多项式

$$a_1f_1(x)+a_2f_2(x)+\cdots+a_rf_r(x)=f(x),\quad a_i\in R$$

其次数都不能超过 n．故可断言：S 不是 $R[x]$ 在 R 上的生成集．

对于 R—模 M 的生成集 S 来说，任一含 S 的 M 的子集 N，都是 M 在 R 上的生成集．我们对不真包含 R—模 M 生成集的生成集，给以特别的重视．

定义 2　设 S 是 R—模 M 的一个生成集，如果 S 的任一个真子集都不是模 M 在环 R 上的生成集，则称 S 为 M 在 R 上的最小生成集．

以上各例中所举的生成集都是最小生成集．这里，例 4 值得我们去注意．对 Z—模 Z_6 所举的两个生成集

$$H=\{\overline{2},\ \overline{3}\},\quad S=\{\overline{1}\}$$

在 H 中有两个真子集：$H_1=\{\overline{2}\}$，$H_2=\{\overline{3}\}$，它们在 Z 上都不能生成 Z_6，故 H 是 Z_6 在 Z 上的最小生成集．S 是只有一个元素构成的集合，没有真子集（非空）．因之 S 也是 Z_6 在 Z 上的最小生成集．Z_6 的这两个最小生成集含有元素的个数不同．

模的最小生成集的概念，是数域上线性空间基底概念的推广．但这一推广，使基底的一些很基本的性质没能承继下来．例如：

（1）在数域F上有限维线性空间V中，任一个基底都含有相同个数的向量；而在环R上的有限生成模M中，不同的最小生成集所含模元素个数可能是不同的．

（2）在数域F上有限维线性空间V中，任一向量x，在基底

$$\{e_1,\ e_2,\ \cdots,\ e_n\}$$

上的表出式

$$x=a_1e_1+a_2e_2+\cdots+a_ne_n,\quad a_i\in F,\quad i=1,\ 2,\ \cdots,\ n$$

是唯一确定的．而对环R上有限生成模M来说，任一模元素x，在最小生成集

$$\{u_1,\ u_2,\ \cdots,\ u_r\}$$

上的表出式

$$x=a_1u_1+a_2u_2+\cdots+a_ru_r,\quad a_i\in R,\quad i=1,2,\cdots,r$$

却不一定唯一．例如，在Z—模Z_6中，对最小生成集

$$H=\{\overline{2},\ \overline{3}\}$$

来说，模元素$\overline{5}\in Z_6$就可表为

$$\overline{5}=1\cdot\overline{2}+1\cdot\overline{3},\ 1\in Z$$

和

$$\overline{5}=4\cdot\overline{2}+5\cdot\overline{3},\ 2、5\in Z$$

这样，对一般的有限生成模来说，就不便引进类似于线性空间中的维数和坐标的概念．因此必须对有限生成模再加以限制条件，才能使不同的最小生成集具有相同的元素个数，才能使任一模元素在最小生成集上有唯一的表出式．这就是下一节所要研究的自由模．

习　　题

1　设R是有$1\neq0$的环，S是一个非空集

$$M=\left\{\sum_{i=1}^{n}a_ix_i \mid a_i\in R,\ x_i\in S\quad \forall n\in N\right\}$$

证明：（1）$\forall\ x=\sum_{i=1}^{n}a_ix_i,\ \ y=\sum_{i=1}^{n}b_ix_i\ \in M$，如果规定

$$x+y=\sum_{i=1}^{n}(a_i+b_i)x_i$$

则M是加群。

（2）$\forall\ r\in R$，再规定

$$rx=\sum_{i=1}^{n}(ra_i)x_i$$

则M是R上的模。

（3）令

$N=\{1x\mid \forall x\in S\}\subseteq M$

则N是M在R上的一个生成集。称R—模M是S在R上的生成模。

2 设 $S_1=\{2\}$，$S_2=\{3\}$，$S_3=\{2,3\}$试求出：S_1，S_2，S_3在整数环$\mathbf{Z}$上的生成模。

如果规定$\mathbf{Z}$乘 $S_i\ \ {}_{i=1,2,3}$的形式乘法有

$1\cdot 2=2$，$1\cdot 3=3$

那么，M_1，M_2，M_3将是环模$\mathbf{Z}$的什么样的子模？

3 设$\mathbf{Z}[\lambda]$是整系数多项式环，$\forall\ f(\lambda)\in\mathbf{Z}[\lambda],x\in\mathbf{Z}$，规定

$f(\lambda)\cdot x=f(x)\in\mathbf{Z}$

则整数加群Z是环$\mathbf{Z}[\lambda]$上的模。证明，$\forall\ y\in\mathbf{Z}$，在 $\mathbf{Z}[\lambda]$上都有

$\mathbf{Z}=L(y)$。

4 设R是有$1\neq 0$的环，$S=(x,\ y)$是R中由标量x和y生成的理想。求：R—模$S^{(2)}=S\oplus S$的生成集。

5 证明，任一有限生成的R—模M，都存在最小生成集。

§3 自 由 模

自由模是比较接近于数域上有限维线性空间的一种模，因而数域上线性空间的一些结果也就便于推广到自由模上。

先谈一下R—模M中元素的线性关系。

对于R—模M，如果$u_1, u_2, \cdots, u_n \in M$，$a_1, a_2, \cdots, a_n \in R$，则称模元素

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n$$

为 $u_1, u_2, \cdots, u_n$ 在R上的一个线性组合。

如果模元素$x \in M$，能表成

$$x = b_1u_1 + b_2u_2 + \cdots + b_nu_n$$

$b_i \in R$，$i = 1, 2, \cdots, n$ 则说x能被模元素 $u_1, u_2, \cdots, u_n$ 线性表出。

显然，模元素θ，一定能被模元素 $u_1, u_2, \cdots, u_n$ 线性表出。因为对任一组模元素 $u_1, u_2, \cdots, u_n$，等式

$$\theta = 0u_1 + 0u_2 + \cdots + 0u_n$$

都必然成立。

对于模元素组 $u_1, u_2, \cdots, u_n$ 来说，如果存在一组不全为零的标量 $a_1, a_2, \cdots, a_n$ 使线性组合式

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = \theta$$

则称模元素组 $u_1, u_2, \cdots, u_n$ 在环R上线性相关。

如果对R中任意一组不全为零的标量，$r_1, r_2, \cdots, r_n$ 线性组合式

$$r_1u_1 + r_2u_2 + \cdots + r_nu_n \neq \theta$$

永远成立，则说模元素组 $u_1, u_2, \cdots, u_n$在环R上线性无关。

模元素组在环R上的线性关系，几乎是向量组在数域上的线性关系的重述。但要注意：由数域推广到环，对线性关系将产生重大影响。

（1）在数域上的线性空间中，一个非零向量一定是线性无关的；而在环上的模中，一个非零模元素则未必是线性无关的。例如

在环模Z_6中，对非零模元素$\overline{2}$来说，用标量$\overline{3}$去倍乘之，则有

$$\overline{3} \cdot \overline{2} = \overline{3 \times 2} = \overline{0}$$

于是知非零元素$\overline{2}$在环Z_6上是线性相关的。

通常将线性无关的模元素叫自由元，否则叫非自由元。

（2）在数域上的线性空间中，一个线性相关的向量组，必存在一个向量能被其余向量线性表出；而在环上的模中，一个线性相关的模元素组，未必存在模元素能被其余模元素线性表出。例如

在环模Z_6中，考查模元素组

$$\{\overline{2},\ \overline{3}\}$$

如果在环Z_6中取标量：$\overline{3}$，$\overline{2}$。再对模元素组作线性组合，则有

$$\overline{3}\cdot\overline{2}+\overline{2}\cdot\overline{3}=\overline{0}$$

于是知$\{\overline{2},\ \overline{3}\}$在环$Z_6$上是线性相关的。但是，模元素$\overline{2}$在环$Z_6$上的倍元集为

$$Z_6\cdot\overline{2}=\{\overline{0},\ \overline{2},\ \overline{4}\}$$

模元素$\overline{3}\in Z_6\cdot\overline{2}$，于是断定模元素$\overline{3}$在环$Z_6$上，不能被模元素$\overline{2}$线性表出。同样，模元素$\overline{3}$在环$Z_6$上的倍元集为

$$Z_6\cdot\overline{3}=\{\overline{0},\ \overline{3}\}$$

模元素$\overline{2}\in Z_6\cdot\overline{3}$，由此推出$\overline{2}$在环$Z_6$上也不能被模元素$\overline{3}$线性表出。

由此断言：在线性相关的模元素组$\{\overline{2},\ \overline{3}\}$中，在环$Z_6$上，任一个模元素都不能被其余模元素线性表出。

还应该注意：模元素组的线性关系，受所在环的制约作用。如将加群Z_6看作环Z_6上的模时，模元素$\overline{1}$是线性无关的；看作整数环$\boldsymbol{Z}$上的模时，有

$$6\cdot\overline{1}=\overline{6\times 1}=\overline{0}$$

$6\in\boldsymbol{Z}$，$6\neq 0$，故知$\overline{1}$在环$\boldsymbol{Z}$上是线性相关的。

定义 1　设R是有$1\neq 0$的环，如果R—模M存在一个线性无关的有限生成集，则称M是R上的自由模。

如果R—模M是自由的，则称它的线性无关的有限生成集为M在R上的自由基。

显然，自由基中任一模元素都是自由元，R—模M的一个自由基，一定是M在R上的一个最小生成集。

以后常将有限集$\{u_1, u_2, \cdots, u_n\}$缩记成$\{u_i\}_{i=1}^n$。

如果R—模M是自由的，自由基为$U=\{u_i\}_{i=1}^n$，则说模M是由自由基U生成的，记为

$$M=\langle u_1\ u_2\ \cdots\ u_n\rangle$$

下述命题是显然的。

假设R—模M是自由的，$U=\{u_i\}_{i=1}^n$是M的一个自由基，则M中任一模元素x都可表为$u_1, u_2, \cdots, u_n$的线性组合

$$x=a_1u_1+a_2u_2+\cdots+a_nu_n$$

并且这种表示法是唯一确定的。

例1　环模Z_6是自由模。因为

$$Z_6=L(\overline{1})$$

且$\overline{1}$在Z_6上是自由的，故$\{\overline{1}\}$是模Z_6在环Z_6上的自由基。$Z_6=\langle\overline{1}\rangle$

例2　Z—模Z_6是非自由模。因为对任一模元素$\overline{a}\in Z_6$，都有$6\in Z$，$6\neq 0$，使

$$6\cdot\overline{a}=\overline{6a}=\overline{0}$$

于是知$\overline{a}$在Z上是非自由的。从而可断言：模Z_6在环Z上的任一生成集都是线性相关的。故知模Z_6在环Z上是非自由的。

例3　设R是有$1\neq 0$的环。

$$R^{(n)}=\{(a_1\ a_2\cdots a_n)\mid a_i\in R\quad i=1,2,\cdots,n\}$$

是由R的加法群作的（外）直和。$\forall\ x=(a_1\ a_2\cdots a_n)\in R^{(n)}$，$r\in R$规定

$$r\cdot x=(ra_1\ ra_2\cdots ra_n)$$

则$R^{(n)}$在代数运算“·”下，构成R上的模。取

$$E=\{e_i\in R^{(n)}\mid e_i=(\overbrace{0\cdots0\,1}^{i}\,0\cdots0),\ i=1,2,\cdots n\}$$

则有$R^{(n)}=L(e_1\ e_2\cdots e_n)$，且当

$$k_1e_1+k_2e_2+\cdots+k_ne_n=\theta$$

$k_i\in R$，$1\leqslant i\leqslant n$时，有$k_i=0$，于是知：E是$R^{(n)}$在R上的线性无关生成集。是$R^{(n)}$在R上的一个自由基。

例4　设R是有$1\neq0$的交换环。

$$R^{(n)}=\{(a_1\ a_2\cdots a_n)\mid a_i\in R,\ 1\leqslant i\leqslant n\}$$

是环R加法群的（外）直和。

$$M_n(R)=\left\{\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \cdot&\cdots&\cdot\\ a_{n1}&\cdots&a_{nn}\end{pmatrix}\middle|\ a_{ij}\in R,\ 1\leqslant i,\ j\leqslant n\right\}$$

是R上的n阶矩阵环。$\forall\ x=(a_1\ a_2\cdots a_n)\in R^{(n)}$，$A=(a_{ij})\in M_n(R)$，规定

$$A\cdot x=xA'$$

则在运算“$\cdot$”下，$R^{(n)}$是环$M_n(R)$上的模，此模是非自由模。

事实上，如果$u=(b_1\ b_2\cdots b_n)\in R^{(n)}$，$u\neq0$，则在$M_n(R)$中存在

$$B=\begin{pmatrix}b_2&-b_1&&&\\ &b_3&-b_2&&\\ &&\ddots&\ddots&\\ &&&b_n&-b_{n-1}\\ -b_n&&&&b_1\end{pmatrix}\neq0$$

使

$$B\cdot u=uB'=\theta$$

于是可知u在$M_n(R)$上是非自由的。所以$R^{(n)}$的任一生成集在环$M_n(R)$上都是线性相关的，从而得知：模$R^{(n)}$在环$M_n(R)$上是非自由的。

在数域F上的有限维空间V中，基底所含向量个数是相同

的，从而导入线性空间维数的概念，下面将这一概念推广到交换环的自由模上。

定理 设R是有$1\neq 0$的交换环，M是R上的自由模。如果$U=\{u_i\}_{i=1}^{n}$和$V=\{v_i\}_{i=1}^{m}$是M在R上的两个自由基，则有$m=n$。

证明 因为U和V是R—模M的两个生成基，故有

$$u_i=\sum_{k=1}^{m}a_{ik}v_k,\quad i=1,2,\cdots,n$$

$$v_j=\sum_{l=1}^{n}b_{jl}u_l,\quad j=1,2,\cdots,m$$

写成阵的形式

$$\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1m}\\a_{21}&a_{22}&\cdots&a_{2m}\\\cdot&\cdot&\cdots&\cdot\\a_{n1}&a_{n2}&\cdots&a_{nm}\end{pmatrix}\begin{pmatrix}v_1\\v_2\\\vdots\\v_m\end{pmatrix}$$

和

$$\begin{pmatrix}v_1\\v_2\\\vdots\\v_m\end{pmatrix}=\begin{pmatrix}b_{11}&b_{12}&\cdots&b_{1n}\\b_{21}&b_{22}&\cdots&b_{2n}\\\cdot&\cdot&\cdots&\cdot\\b_{m1}&b_{m2}&\cdots&b_{mn}\end{pmatrix}\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}$$

会看得更清楚些。于是有

$$\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}=AB\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}$$

和

$$\begin{pmatrix}v_1\\v_2\\\vdots\\v_m\end{pmatrix}=BA\begin{pmatrix}v_1\\v_2\\\vdots\\v_m\end{pmatrix}$$

其中 $A=(a_{ij})$ 是 R 上的 n 行 m 列阵，$B=(b_{ij})$ 是 R 上 m 行 n 列阵。故知：AB 是 R 上 n 阶方阵；BA 是 R 上 m 阶方阵。再由 $\{u_i\}_{i=1}^n$ 和 $\{v_j\}_{j=1}^m$ 是模 M 在 R 上的线性无关组。进而断定

$$AB=E_n,\quad BA=E_m$$

不妨假定 $m<n$，可将 A 补成 n 阶方阵

$$A_1=\begin{pmatrix} a_{11} & \cdots & a_{1m} & 0 & \cdots & 0 \\ a_{21} & \cdots & a_{2m} & 0 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ a_{n1} & \cdots & a_{nm} & 0 & \cdots & 0 \end{pmatrix}=(A\quad O_{n\times(n-m)})$$

将 B 也补成 n 阶方阵

$$B_1=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ \cdot & \cdot & \cdots & \cdot \\ b_{m1} & b_{m2} & \cdots & b_{mn} \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 0 \end{pmatrix}=\begin{pmatrix} B \\ O_{(n-m)\times n} \end{pmatrix}$$

于是有

$$A_1B_1=(A\ O)\begin{pmatrix} B \\ O \end{pmatrix}=AB=E_n$$

A_1 和 B_1 是有 1 交换环 R 上的 n 阶可逆阵，据第三章 § 4 可知

$$B_1A_1=A_1B_1=E_n$$

但是

$$B_1A_1=\begin{pmatrix} B \\ O \end{pmatrix}(AO)=\begin{pmatrix} BA & O \\ O & O \end{pmatrix}\neq E_n$$

矛盾。故知 $m\geqslant n$；同理可证，$n\geqslant m$，所以只能有 $m=n$，证完。

定义 2　设 R 是有 $1\neq 0$ 的交换环，M 是 R 上的自由模。称 M 在 R 上的自由基所含模元素的个数 n 为模 M 在 R 上的秩。此时称 M 为 R 上的 n 秩自由模。

习　　题

1　设$\{x_1,x_2,\cdots,x_m\}$是R—模M的一个线性无关组，$\{x_1,x_2,\cdots,x_m,x_{m+1}\}$是$R$—模$M$的一个线性相关组。那么$x_{m+1}$一定能被$x_1,x_2,\cdots,x_m$线性表出吗？如果$R$是除环，结果将如何？

2　证明：环R上自由模M的自由基$U=\{u_i\}_{i=1}^n$一定是M在R上的最小生成集。

3　设R是有$1\neq0$的交换环，所有非单位（非可逆元）都含在真理想N中，考查R—模$R^{(n)}$。令$U=\{u_i=(a_{i1},a_{i2},\cdots,a_{in})\}_{i=1}^n$是$R^{(n)}$的$R$—自由基，则

（1）$Ru_i=\{au_i\mid a\in R\}$，$\forall\ u_i\in U$。

按R—模$R^{(n)}$的运算，构成1秩自由模。

（2）$a_{ij},j=1,2,\cdots,n$中至少有一个元素是R中的单位(可逆元) $1\leqslant i\leqslant n$

（3）$a_{i1},a_{i2},\cdots,a_{in}$生成的理想

$$\langle a_{i1},a_{i2},\cdots,a_{in}\rangle=R$$

（4）$\overline{a_{ij}}=a_{ij}+N$在$R/N$中，至少有一个是单位（可逆元）。

4　设　$R=\{a+bi\mid a,b\in\mathbf{Z}\}=\mathbf{Z}[i]$。对于$R$—模$R^{(n)}$和$\mathbf{Z}$—模$R^{(n)}$

（1）$R^{(n)}$中任一个R—线性无关组也是$\mathbf{Z}$—线性无关吗？

（2）$R^{(n)}$中任一个R—线性相关组也是$\mathbf{Z}$—线性相关吗？

（3）$R^{(n)}$在R上是n秩自由模，在$\mathbf{Z}$上也是自由的吗？如果是，秩数是多少？

5　设M_1和M_2是R上的两个自由模，秩数分别是n_1和n_2。令

$$M=M_1\oplus M_2=\{(a_1,a_2)\mid a_1\in M_1,a_2\in M_2\}$$

是M_1和M_2的（外）直和所作的加群。$\forall\ r\in R$，$(a_1,a_2)\in M$，如果规定

$$r(a_1,a_2)=(ra_1,ra_2)$$

则M构成R上的模，称R—模M为R—模M_1和R—模M_2的(外)直和。证明，

（1）R—模M是自由模；

（2）R—模M的秩$n=n_1+n_2$。

6　R是环Q的子环。M是R上的自由模，试问：M是否是Q上的模？

如果R是Q的理想其结果又如何？

§4　n 秩自由模上的线性代数

有$1\neq 0$的交换环上n秩自由模与数域上n维线性空间比较，仅差一个标量可除性条件．因此，在把数域上n维线性空间的结果向交换环上n秩自由模推广时，注意到不可除性就可以了．

设R是有$1\neq 0$的交换环，M是R上的n秩自由模，$U=\{u_i\}_{i=1}^n$是M的R—自由基．由U是M在R上的生成集，可知$\forall x\in M$，在R上一定存在有序标量组：$(a_1, a_2, \cdots, a_n)$，$a_i\in R_{i=1,2,\cdots,n}$使

$$x=a_1u_1+a_2u_2+\cdots+a_nu_n$$

又由于U在R上是线性无关的，可知有序标量组$(a_1, a_2, \cdots, a_n)$是唯一确定的．称有序标量组$(a_1,a_2,\cdots,a_n)$为模元素x在R—自由基U上的坐标，记作：$[x]_U=(a_1, a_2,\cdots,a_n)$．

对于M上的模元素x，y和R上的标量r如果

$$[x]_U=(a_1,a_2,\cdots,a_n)$$

$$[y]_U=(b_1,b_2,\cdots,b_n)$$

规定

$$[x]_U+[y]_U=(a_1+b_1,\ a_2+b_2,\cdots,a_n+b_n)$$

$$r[x]_U=(ra_1,\ ra_2,\ \cdots,ra)$$

则有

$$[x+y]_U=[x]_U+[y]_U$$

$$[rx]_U=r[x]_U$$

由于模元素在自由基U上的坐标由自由基的确定而确定，所以当自由基改换时，一般说来同一模元素的坐标也将随之改换．二自由基间的改换规律由下述定理给出．

定理 1　**设M是环R上的n秩自由模，$U=\{u_i\}_{i=1}^n$是M在R上的自由基．则模元素集**

$$V=\{v_i\in M\mid [v_i]_U=(a_{i1},a_{i2},\cdots,a_{in})\}$$

是M在R上的自由基必要而且只要矩阵

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \cdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

在R上是可逆的。称矩阵A为自由基U到自由基V的演化阵。

证明　必要性。当$V=\{v_i\}_{i=1}^n$是M在R上的自由基时，将有$B=(b_{ij})\in M_n(R)$，使

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}=B\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

其中　$[u_i]_V=(b_{i1},\ b_{i2},\ \cdots,\ b_{in})$。由定理条件可知

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}=A\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

于是有

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}=BA\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

由U是自由基，可断定$BA=E$。于是由第三章§4可知A是R上的可逆阵。

充分性。若A是R上n阶可逆阵，则在R上存在n阶阵B，使$AB=BA=E$。于是有

$$B\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}=BA\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}=\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}$$

故知：$\forall x\in M$，将有

$$x=[x]_U\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}=[x]_UB\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}$$

$V=\{v_i\}_{i=1}^n$ 是M在R上的一个生成集。又，如果

$$(a_1\ a_2\ \cdots\ a_n)\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}=\theta$$

$a_i\in R(i=1,\ 2,\ \cdots,\ n)$ 则

$$(a_1\ a_2\ \cdots\ a_n)A\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}=\theta$$

由于U是自由基，于是得

$$(a_1\ a_2\ \cdots\ a_n)A=(0\ 0\ \cdots\ 0)$$

从而有

$$\begin{aligned}(a_1\ a_2\ \cdots\ a_n)&=(a_1\ a_2\ \cdots\ a_n)(AB)\\&=[(a_1\ a_2\ \cdots\ a_n)A]B\\&=(0\ \ 0\ \cdots\ 0)B\\&=(0\ \ 0\ \cdots\ 0)\end{aligned}$$

即 $V=\{v_i\}_{i=1}^n$ 是M在R上的线性无关元素组。所以，V是M在R上的一个自由基。证完。

下面再看一下，自由基间的相互演化对模元素坐标影响规律。

定理 2　设 $U=\{u_i\}_{i=1}^n$ 和 $V=\{v_i\}_{i=1}^n$ 是 R 上 n 秩自由模 M 的两个自由基，且

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = A \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

则，$\forall x \in M$ 都有

$$[x]_U = [x]_V A$$

证明　因为

$$[x]_V \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = x = [x]_U \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

于是有

$$[x]_V A \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = [x]_U \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

由于 U 是自由基，故有

$[x]_U = [x]_V A$，证完。

定义 1　设 M 是环 R 上的 n 秩自由模，

$$\varphi: M \to M$$

是加群 M 的自同态，如果满足

$$\varphi(rx) = r\varphi(x), \quad \forall x \in M, \ r \in R$$

则称 φ 是模M上的 R—自同态。

例 1　R 上 n 秩自由模 M 的恒等变换

$$I_M(x) = x$$

$\forall x \in M$，是 M 上的 R—自同态。

例 2　R 上 n 秩自由模 M 的位似变换

$$L_a(x) = ax, \quad a \in R, \quad \forall x \in M$$

是M上的R—自同态。

例 3 M是环R上的n秩自由模。ρ是M上的一个线性型，即 $\rho: M \to R$，且满足

$$\rho(x+y) = \rho(x) + \rho(y)$$
$$\rho(rx) = r\rho(x),$$

$\forall x, y \in M$，$r \in R$对$u \in M$，规定

$$\tau_{\rho,u}(x) = x + \rho(x)u, \quad \forall x \in M$$

则$\tau_{\rho,u}$是M上的R—自同态（叫做由线性型ρ和模元素u所定义的线性平延）。

解 $\forall\ x, y \in M$，有

$$\begin{aligned}\tau_{\rho,u}(x+y) &= (x+y) + \rho(x+y)u \\ &= (x+y) + [\rho(x) + \rho(y)]u \\ &= [x + \rho(x)u] + [y + \rho(y)u] \\ &= \tau_{\rho,u}(x) + \tau_{\rho,u}(y)\end{aligned}$$

于是知 $\tau_{\rho,u}$是加群M的自同态。又 $\forall\ x \in M$，$r \in R$，有

$$\begin{aligned}\tau_{\rho,u}(rx) &= rx + \rho(rx)u \\ &= rx + r\rho(x)u \\ &= r[x + \rho(x)u] \\ &= r\tau_{\rho,u}(x)\end{aligned}$$

于是知 $\tau_{\rho,u}$是M的R—自同态。

定义 2 设M是环R上的n秩自由模，$U = \{u_i\}_{i=1}^{n}$是M的R—自由基。φ是M上的R—自同态，如果

$$[\varphi(u_i)]_U = (a_{i1}\ a_{i2} \cdots a_{in})$$

$i = 1, 2, \cdots, n$，则称阵

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

为R—自同态φ在R—自由基U上的阵。记作 $A = \mathrm{Mat}_U\varphi$。

对φ来说，$\mathrm{Mat}_U\varphi$是唯一确定的。

例 4 n 秩自由模M上的恒等变换I_M，在M的任一自由基U上的阵，都是单位阵。即

$$\mathrm{Mat}_U I_M = E = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

例 5 n 秩自由模M上的位似变换L_a，在M的任一自由基U上的阵都是纯量阵。即

$$\mathrm{Mat}_U L_a = aE = \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}$$

例 6 n 秩自由模M上的由线性型ρ和模元素u定义的线性平延$\tau_{\rho,u}$，在R—自由基$U=\{u_i\}_{i=1}^n$上，如果 $\rho(u_i)=a_i$，$[u]_U=(b_1\ b_2\cdots b_n)$，则

$$\mathrm{Mat}_U(\tau_{\rho,u}) = \begin{pmatrix} 1+a_1b_1 & a_1b_2 & \cdots & a_1b_n \\ a_2b_1 & 1+a_2b_2 & \cdots & a_2b_n \\ \cdot & \cdot & \cdots & \cdot \\ a_nb_1 & a_nb_2 & \cdots & 1+a_nb_n \end{pmatrix}$$

$$= E + \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} (b_1\ b_2\cdots b_n)$$

解 由 $\tau_{\rho,u}(u_i)=u_i+\rho(u_i)u$，于是得

$$[\tau_{\rho,u}(u_i)]_U = [u_i]_U + a_i[u]_U$$
$$= (a_ib_1\cdots(1+a_ib_i)\cdots a_ib_n)$$

$i=1,2,\cdots,n$，从而得

$$\mathrm{Mat}_U\,\tau_{\rho,\alpha}=\begin{pmatrix}1+a_1b_1 & a_1b_2 & \cdots & a_1b_n\\ a_2b_1 & 1+a_2b_2 & \cdots & a_2b_n\\ \cdot & \cdot & \cdots & \cdot\\ a_nb_1 & a_nb_2 & \cdots & 1+a_nb_n\end{pmatrix}$$

$$=E+\begin{pmatrix}a_1\\ a_2\\ \vdots\\ a_n\end{pmatrix}(b_1\ \ b_2\cdots b_n)$$

R一自同态φ的阵$\mathrm{Mat}_U(\varphi)$由R一自由基U所唯一确定。下面看一下自由基间的相互演化对φ的阵的影响规律。

定理 3 设R一模M是n秩自由模，$U=\{u_i\}_{i=1}^n$ 和 $V=\{v_i\}_{i=1}^n$ 是M的两个R一自由基，且

$$\begin{pmatrix}v_1\\ v_2\\ \vdots\\ v_n\end{pmatrix}=C\begin{pmatrix}u_1\\ u_2\\ \vdots\\ u_n\end{pmatrix}$$

$C=(C_{ij})\in M_n(R)$，是自由基U到V的演化阵。如果M上R一自同态φ在U上的阵是A，在V上的阵是B，则

$$B=CAC^{-1}$$

证明 $\forall\ x\in M$，由φ在V上的阵是B， 可知

$$[\varphi(x)]_V=[x]_VB$$

由φ在U上的阵是A，可知

$$[\varphi(x)]_U=[x]_UA$$

又因为

$$[\varphi(x)]_U=[\varphi(x)]_VC$$

$$[x]_U=[x]_VC$$

于是得到

$$[x]_VBC=[x]_UA=[x]_VCA$$

由于$\forall\ x\in M$ 上式皆成立，故有

$$BC = CA$$

从而得出：$B = CAC^{-1}$.证完。

下面讨论一下R—自态的集合。设R—模M是n秩自由模。令

$$\mathrm{End}_R(M) = \{\phi: M \to M \mid \varphi \text{是} R\text{—自同态}\}$$

（1）$\forall\ \varphi, \psi \in \mathrm{End}_R(M)$，规定

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x), \quad \forall\ x \in M$$

则$\{\mathrm{End}_R(M), +\}$是加群。称为R—自由模M上的R—自同态加群。此群的零元为

$$0(x) = \theta, \quad \forall\ x \in M$$

称为零变换。

（2）$\forall\ \varphi \in \mathrm{End}_R(M)$，$r \in R$，规定

$$(r \cdot \varphi)(x) = r(\varphi(x)), \quad \forall\ x \in M$$

则加群$\{\mathrm{End}_R(M), +\}$构成环R上的n^2秩自由模。

这只要证明：R—模$\mathrm{End}_R(M)$存在着n^2个模元素构成的R—自由基即可。

事实上，令$U = \{u_i\}_{i=1}^n$为R—模M的一个自由基，取M上的R—自同态

$$\rho_{ij}: M \to M$$

$$x = \sum_{i=1}^n a_i u_i \longmapsto a_i u_j \quad \forall\ x \in M$$

即：$\rho_{ij} x = a_i u_j$.可以验证

$$P = \{\rho_{ij}\}_{1 \le i, j \le n}$$

是R—模$\mathrm{End}_R(M)$的一个R—自由基.这是因为，当$\varphi \in \mathrm{End}_R(M)$时，有$\mathrm{Mat}_U(\varphi) = (a_{ij}) \in M_n(R)$，对$x = \sum_{i=1}^n a_i u_i \in M$，有

$$\varphi(x) = \varphi\left(\sum_{i=1}^n a_i u_i\right) = \sum_{i=1}^n a_i \varphi(u_i)$$

$$= \sum_{i=1}^n a_i\left(\sum_{j=1}^n a_{ij} u_j\right) = \sum_{i=1}^n \sum_{j=1}^n a_{ij}(a_i u_j)$$

$$=\left(\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}\rho_{ij}\right)x$$

$\forall x\in M$，上式皆成立，于是有

$$\varphi=\sum_{i=1}^{n}\sum_{j=1}^{n}a_{ij}\rho_{ij}$$

所以 $P=\{\rho_{ij}\}_{1\leqslant i,j\leqslant n}$ 是 $\text{End}_R(M)$ 在 R 上的一个生成集，又因为，当

$$\sum_{i=1}^{n}\sum_{j=1}^{n}r_{ij}\rho_{ij}=0\text{（变换）}$$

时，则 $\forall\ u_k\in U$ 都有

$$\sum_{i=1}^{n}\sum_{j=1}^{n}r_{ij}\rho_{ij}(u_k)=0(u_k)=\theta$$

于是由 ρ_{ij} 的规定可得

$$\sum_{j=1}^{n}r_{kj}u_j=\theta$$

由此得：$r_{kj}=0\ (j=1,2,\cdots,n)$；对$1\leqslant k\leqslant n$都成立，从而知 $P=\{\rho_{ij}\}_{1\leqslant i,j\leqslant n}$ 在 R 上是线性无关的元素组。所以 P 是 R—模$\text{End}_R(M)$ 的一个自由基。$\text{End}_R(M)$ 是 R 上n^2**秩自由模**。

（3）$\forall\varphi,\ \psi\in\text{End}_R(M)$：规定

$$(\varphi\circ\psi)x=\varphi(\psi(x))\quad\forall\ x\in M$$

则$\{\text{End}_R(M),\ +,\ \circ\}$是环，称为**模$M$的$R$—自同态环**。

（4）$\forall\varphi,\ \psi\in\text{End}_R(M),\ r\in R$ 有

$$(r\cdot\varphi)\circ\psi=\varphi\circ(r\cdot\psi)=r\cdot(\varphi\circ\psi)$$

综合上述，可知自由模M上的 R—自同态环 $\{\text{End}_R(M),\ +,\ \circ\}$和环$R$，在代数运算“$\cdot$”下组成一个代数体系。这是一个比模的条件更加复杂的代数体系。此代数体系叫做环R上的**线性变换代数**。

“代数”一词，指的是具有一定运算结构的代数体系。它与代数学科中“代数”一词，具有不同的含义。

下面再看一下环R上的线性变换代数用环R上的矩阵来表

示的问题。

对于R上的矩阵环$M_n(R)$，也有R中元素r对$M_n(R)$中矩阵$A=(a_{ij})$的乘法运算

$$rA=(ra_{ij})\in M_n(R)$$

这时矩阵环$M_n(R)$与环R在此运算下也构成一个代数体系，叫做环R上的n阶矩阵代数。

设R是有$1\neq 0$的交换环。M是R上的n秩自由模，$U=\{u_i\}_{i=1}^n$是M的一个R—自由基。令

$$\mathrm{Mat}_U:\ \mathrm{End}_R(M)\longrightarrow M_n(R)$$
$$\varphi\longmapsto \mathrm{Mat}_U\varphi\in M_n(R)$$

$\forall\varphi\in\mathrm{End}_R(M)$，则$\mathrm{Mat}_U$是双射，且满足

（1）$\mathrm{Mat}_U(\varphi+\psi)=\mathrm{Mat}_U\varphi+\mathrm{Mat}_U\psi$

（2）$\mathrm{Mat}_U(a\varphi)=a(\mathrm{Mat}_U\varphi)$

（3）$\mathrm{Mat}_U(\varphi\psi)=(\mathrm{Mat}_U\psi)(\mathrm{Mat}_U\varphi)$

$\forall\ \varphi,\psi\in\mathrm{End}_R(M)$，$a\in R$。

其中（1），（2）是易证的．下面证一下（3）．对于$x\in M$，有

$$[(\varphi\psi)x]_U=[x]_U\mathrm{Mat}_U(\varphi\psi)$$

和

$$[\varphi(\psi x)]_U=[\psi(x)]_U\mathrm{Mat}_U\varphi$$
$$=\{[x]_U Mat_U\psi\}\mathrm{Mat}\varphi$$
$$=[x]_U[\mathrm{Mat}_U\psi\,\mathrm{Mat}_U\varphi]$$

由于$(\varphi\psi)(x)=\varphi(\psi(x))$，故知

$$[x]_U\mathrm{Mat}_U(\varphi\psi)=[x]_U[\mathrm{Mat}_U\psi\mathrm{Mat}_U\varphi]$$

对任一$x\in M$都成立，于是得

$$\mathrm{Mat}_U(\varphi\psi)=(\mathrm{Mat}_U\psi)(\mathrm{Mat}_U\varphi)$$

此时称环R上的代数$\mathrm{End}_R(M)$与$M_n(R)$，在映射Mat_U下，是反同构代数。在同构前冠以“反”字是说φ与ψ之积在Mat_U下之象，为φ与ψ在Mat_U之下象的反序积。

R上的代数$M_n(R)$是用R中元素做出来的。比R上以M

的自同态为元素的代数$\mathrm{End}_R(M)$来说，更为具体和明确。因此对一些课题，往往是放在代数 $M_n(R)$ 中去研究，其结论相应的在代数 $\mathrm{End}_R(M)$中也成立。通常将R—代数 $M_n(R)$作为R—代数$\mathrm{End}_R(M)$的表示来使用。“高等代数”中用系数阵去研究线性变换，就是这一思想的体现。

习　　题

1　试求出环模 $\mathbf{Z}_6$的所有自由基及两两自由基间的演化阵，并对模元素$\overline{2}$，$\overline{3}$求出在各自由基上的坐标。

2　求出$\mathbf{Z}$—模$\mathbf{Z}^{(2)}$的两个自由基，并求出模元素$(1,-1)$，$(0,2)$，$(5,7)$在所求自由基上的坐标。

3　对$\mathbf{Z}$—模$\mathbf{Z}^{(n)}$ 的子集

$$U=\{a_i=(a_{i1},a_{i2}\cdots a_{in})\in\mathbf{Z}^{(n)}\mid i=1,2,\cdots,n\}$$

证明：U是 $\mathbf{Z}^{(n)}$ 在$\mathbf{Z}$上的自由基，必要而且只要阵 $A=(a_{ij})$ 的行列式 $\det A=\pm1$。

4　设　$R=\{a+bi\mid a,\ b\in\mathbf{Z},\ i^2=-1\}$是高斯环，$M=R^{(3)}$，对$R$—自由模$M$

（1）求出M的两个R—自由基U和V

（2）已知R—自同态φ，ψ具有

$$\mathrm{Mat}_U(\varphi)=\begin{pmatrix}1&0&i\\0&1&0\\0&0&1\end{pmatrix}$$

$$\mathrm{Mat}_V(\psi)=\begin{pmatrix}i&0&0\\0&-i&0\\0&0&1\end{pmatrix};$$

试求R—自同态

$$f(\varphi,\psi)=I_M+\varphi+\psi+\varphi\psi$$

在自由基U上的阵。

5　设　$M=\left\{\sum_{i=1}^{n}a_i x^i\mid a_i\in\mathbf{R}\right\}$。对于$\mathbf{R}$—模$M$（$\mathbf{R}$是实数域）

（1）D是微分算子，证明：$D^{n+1}=0$，并求出在R—自由基 $U=\{x^i\}_{i=0}^n$ 和 $V=\left\{\frac{x^i}{i!}\right\}_{i=0}^n$上的阵。

（2）令 φ：$f(x)\mapsto f(x+1)$，$\forall f(x)\in M$，证明：φ是R—自同态，且有

$$\varphi=\varepsilon+\frac{D}{1!}+\frac{D^2}{2!}+\cdots+\frac{D^n}{n!}$$

（3）决定R—自同态 $\delta=\varphi-I_M$ 在自由基：

$$W=\left\{\omega_i=\frac{x(x-1)\cdots(x-i+1)}{i!},\ \omega_0=1,\middle|_{i=1,2,\cdots,n}\right\}$$

上的阵。

6　对于R—n 秩自由模M

（1）证明：R—模$\mathrm{End}_R(M)$是n^2秩的自由模。

（2）求出 R—模$\mathrm{End}_R(M)$ 的两个R—自由基。

（3）如果 $\varphi\in\mathrm{End}_R(M)$，且在某自由基$U$上有 $Mnd_U(\varphi)=A=(a_{ij})$，试求$\varphi$在(2)中所求的$R$—自由基上的坐标。

§5　向量空间上的线性代数

一般环上的模是比较复杂的，为了便于将数域上线性空间的一些结果推广到环上的模，在§4中将一般的模强化成交换环上n秩自由模，在此基础上讨论了交换环R上的线性变换代数$\mathrm{End}_R(M)$。

本节将把模的一般条件强化为除环上的有限生成模。这时情况要简单些，这是由于有

定理1　除环K上的有限生成左模V都存在K—自由基。

证明　设S是V在K上的一个有限生成集，则在S中可选出一个最小生成集

$$X=\{x_i\}_{i=1}^n\subseteq S$$

对K中任一组不全为零的标量 $b_1,b_2,\cdots,b_n$，都有

$$b_1x_1+b_2x_2+\cdots+b_nx_n\neq\theta$$

否则，若

$$b_1x_1+b_2x_2+\cdots+b_nx_n=\theta$$

且有 $b_i\neq 0$，那么将有

$$x_i=(-b_i^{-1}b_1)x_1+\cdots+(-b_i^{-1}b_{i-1})x_{i-1}+$$
$$(-b_i^{-1}b_{i+1})x_{i+1}+\cdots+(-b_i^{-1}b_n)x_n$$

于是 $X'=\{x_1,\ \cdots,\ x_{i-1},\ x_{i+1},\ \cdots,\ x_n\}$ 也是V在K上的一个生成集，且有 $X'\subset X$，这与X是最小生成集矛盾。从而知 X 是V在K上的一个线性无关的有限生成集，X是V在 K 上的自由基。证完。

定义 1　除环 K 上有限生成左(右)模，称为 K 上左（右）向量空间；K—自由基简称 K—基；K 中元素称为纯量，V 中元素称为向量。

例 1　设 K 是除环，则 K—模 $K^{(3)}$是一个 K 上向量空间，这里

$$K^{(3)}=\{(a_1\ \ a_2\ \ a_3)\mid a_i\in K,\ i=1,2,3\}$$

是加群 K 的（外）直和。作用乘法为

$$kx=k(a_1\ \ a_2\ \ a_3)=(ka_1\ \ ka_2\ \ ka_3)$$

$\forall x\in K^{(3)}$，$k\in$ K，此向量空间是K上的左空间。

相当于维数定理有

定理 2　设 V 是除环 K 上的左向量空间，如果 $X=\{x_i\}_{i=1}^{n}$，$Y=\{y_i\}_{i=1}^{m}$ 是 V 的两个 K—基，则有 $m=n$。

证明　若$m\neq n$，不妨假定 $m>n$。考查向量组

$$Y_1=\{y_1,\ x_1,\ \cdots,\ x_n\}\supseteq X$$

由X是K—基，知Y_1是线性相关的，故存在不全为零的纯量：b_1，a_1，$\cdots$，a_n使

$$b_1y_1+a_1x_1+\cdots+a_nx_n=\theta$$

易知$b_1\neq 0$，于是 a_i，$_{1\leqslant i\leqslant n}$，中至少有一个不为 0，不妨设 $a_n\neq 0$，于是有

$$x_n=-a_n^{-1}(b_1y_1+a_1x_1+\cdots+a_{n-1}x_{n-1})$$

从而知

$$Y_1' = \{y_1, x_1, \cdots, x_{n-1}\}$$
仍是V在K上的生成集，于是知
$$Y_2 = \{y_1, y_2, x_1, \cdots, x_{n-1}\}$$
是V在K上的线性相关组。从而知在K中存在不全为零的纯量：$c_1, c_2, d_1, \cdots, d_{n-1}$使
$$c_1y_1 + c_2y_2 + d_1x_1 + \cdots + d_{n-1}x_{n-1} = \theta$$
易知c_1，c_2不全为零，故$d_{i(1\leq i\leq n-1)}$不能全为0，不妨设$d_{n-1} \neq 0$，于是有
$$x_{n-1} = -d_{n-1}^{-1}(c_1y_1 + c_2y_2 + d_1x_1 + \cdots + d_{n-2}x_{n-2})$$
从而知
$$Y_2' = \{y_1, y_2, x_1, \cdots, x_{n-2}\}$$
仍是V在K上的生成集，如此下去，由 $m>n$，得到V在K上的生成集
$$Y_n' = \{y_1, y_2, \cdots, y_n\} \subset Y = \{y_1, \cdots, y_n, y_{n+1}, \cdots, y_m\}$$
这与Y是V的K—基矛盾，故$m \not> n$，同理，$m \not< n$，于是$m = n$。

由此给出除环上左（右）向量空间维数定义

定义 2　除环K上左（右）向量空间V的K—基所含向量的个数n，称为V在K上的维数，这时，称V为K上的n维左（右）向量空间。

不特殊声明时，以后称"K上的向量空间"，总是指K上的左向量空间。

例 2　除环K上向量空间$K^{(3)}$中（参看例 1）
$$U = \{e_1 = (1,0,0),\ e_2 = (0,1,0),\ e_3 = (0,0,1)\}$$
是$K^{(3)}$的一个K—基。其中含三个向量，故$K^{(3)}$在K上是 3 维的。

对于除环K上的向量空间V，设 $X = \{x_i\}_{i=1}^n$ 是它的一个K—基。则$\forall x \in V$，都有一组纯量：$k_1, k_2, \cdots, k_n \subset K$，使
$$x = k_1x_1 + k_2x_2 + \cdots + k_nx_n$$
称有序纯量组$(k_1, k_2, \cdots, k_n)$为向量x在K—基X上的坐标。记作

$$[x]_X=(k_1,\ k_2,\ \cdots,\ k_n)$$

$\forall x,\ y\in V,\ k\in K$，当$[x]_X=(k_1,\ k_2,\ \cdots,\ k_n)$，$[y]_X=(l_1,l_2,\cdots,l_n)$时，如果规定

$$[x]_X+[y]_X=(k_1+l_1,\ k_2+l_2,\ \cdots,\ k_n+l_n)$$

$$k[x]_X=(kk_1,\ kk_2,\ \cdots,\ kk_n)$$

则有

$$[x+y]_X=[x]_X+[y]_X,\quad [kx]_X=k[x]_X$$

因此向量的运算可以通过坐标的运算来实现.

在除环K的向量空间中，K—基间演化规律为

定理 3　设V是除环K上的n维向量空间，$X=\{x_i\}_{i=1}^n$是V的K—基. 则向量组

$$Y=\{y_i\in V\mid[y_i]_X=(c_{i1},c_{i2},\cdots c_{in}),\ i=1,2,\cdots,n\}$$

是V的K—基，必要而且只要

$$C=\begin{pmatrix}c_{11} & c_{12} & \cdots & c_{1n}\\ c_{21} & c_{22} & \cdots & c_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ c_{n1} & c_{n2} & \cdots & c_{nn}\end{pmatrix}$$

是K上的可逆阵. 此时，称阵C为K—基X到K—基Y的演化阵.

此定理可仿“高等代数”中有关定理加以证明.

例 3　在K—向量空间$K^{(3)}$中，对K—基

$$U=\{e_1=(1,0,0),\ e_2=(0,1,0),\ e_3=(0,0,1)\}$$

用可逆阵

$$C=\begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

作演化阵，可得$K^{(3)}$的新K—基$F=\{f_i\}_{i=1}^3$

$$\begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} = \begin{pmatrix} e_1+e_3 \\ e_2 \\ e_3 \end{pmatrix}$$

于是得

$$F=\{f_1=(1\ 0\ 1),\ f_2=(0\ 1\ 0),\ f_3=(0\ 0\ 1)\}$$

除环 K 上的向量空间中，K—基的相互演化，对向量 x 坐标影响规律为

定理 4 在除环 K 上向量空间 V 中，如果 K—基 $X=\{x\}_{i=1}^{n}$ 到 K—基 $Y=\{y_i\}_{i=1}^{n}$ 的演化阵为 C，$x\in V$，则

$$[x]_X=[x]_Y C$$

此定理的证明作为练习。

例 4 在 K—向量空间 $K^{(3)}$ 中，K—基 U 到 K—基 F 的演化阵为

$$C=\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

（参看例 3），$x=(2\ 3\ -5)\in K^{(3)}$，则

$$[x]_U=(2\quad 3\quad -5)$$

于是有

$$[x]_F=(2\ 3\ -5)\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}=(2\ 3\ -7)\text{.}$$

定义 3 设 V 是除环 K 上的向量空间，φ 是 V 上的变换。如果满足

（1）$\varphi(x+y)=\varphi(x)+\varphi(y)$

（2）$\varphi(kx)=k\varphi(x)$，$\forall x,\ y\in V,\ k\in K$

则称 φ 为 V 上的线性变换。

（1）是说 φ 是加群 V 的自同态变换，（2）是说倍乘纯

量因子 k，在 φ 下是可以析出的。所以 V 上的线性变换 φ，就是K—模 V 上的K—自同态。

例 5 除环 K 上向量空间 V 的零变换

$$O(x)=\theta,\quad \forall x\in V$$

和恒等变换

$$I_V(x)=x,\quad \forall x\in V$$

都是 V 上的线性变换。

例 6 设 K 是除环，$C(K)$ 是 K 的中心，$a\in C(K)$，V 是 K 上的向量空间，位似变换

$$La(x)=ax,\quad \forall x\in V$$

是 V 上线性变换。

例 7 除环 K 上向量空间$K^{(3)}$ 中，镜面反射

$$\varphi_1(x)=(k_1,\ k_2,\ -k_3)$$

$\forall x=(k_1,\ k_2,\ k_3)\in K^{(3)}$，和射影

$$\varphi_2(x)=(k_1,\ k_2,\ 0)$$

$\forall x=(k_1,\ k_2,\ k_3)\in K^{(3)}$，都是线性变换。

下面再研究一下，线性变换在 K—基上的矩阵表示。

设 V 是除环 K 上的向量空间，$X=\{x_i\}_{i=1}^n$ 是 V 的K—基，φ 是 V 上的线性变换。如果

$$[\varphi(x_i)]_X=(a_{i1}\ a_{i2}\ \cdots\ a_{in})$$

$i=1,2,\cdots,n$，则称阵

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdot & \cdot & \cdots & \cdot\\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}$$

为线性变换 φ 在K—基X上的阵。记作

$$\mathrm{Mat}_X(\varphi)=A$$

显然，φ 在K—基X上的阵是唯一确定的，此时$\forall\ x=\sum_{i=1}^{n}b_ix_i$

$\in V$，有

$$[\varphi(x)]_X=\left[\varphi\left(\sum_{i=1}^{n}b_i x_i\right)\right]_X=\left[\sum_{i=1}^{n}b_i\varphi(x_i)\right]_X$$

$$=\sum_{i=1}^{n}b_i[\varphi_i[x_i]]_X=\sum_{i=1}^{n}b_i(a_{i1}\ a_{i2}\ \cdots\ a_{in})$$

$$=(b_1\ b_2\ \cdots\ b_n)\begin{pmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \cdot & \cdot & \cdots & \cdot\\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}$$

于是得

$$[\varphi(x)]_X=[x]_X\,\mathrm{Mat}_X(\varphi)$$

这就是线性变换 φ 在 K—基X上的矩阵表示式。

例 8 除环K上向量空间V的零变换 0，在V的任一K—基上的阵都是零阵

$$\mathbf{0}=\begin{pmatrix}0 & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0\\ \cdot & \cdot & \cdots & \cdot\\ 0 & 0 & \cdots & 0\end{pmatrix}$$

恒等变换 I_V 在V的任一K—基上的阵都是单位阵

$$E=\begin{pmatrix}1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}$$

例 9 除环K上向量空间V的、由K的中心元素 a 决定的位似变换

$$L_a(x)=ax,\quad \forall x\in V$$

在V的任一K—基上的阵都是纯量阵。

$$aE=\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}$$

例10 除环 K 上向量空间 $K^{(3)}$ 的镜面反射

$$\varphi(x)=(k_1\ k_2\ -k_3),\quad \forall x=(k_1\ k_2\ k_3)\in K^{(3)}$$

关于 K—基 $U=\{e_1=(1\ 0\ 0),\ e_2=(0\ 1\ 0),\ e_3=(0\ 0\ 1)\}$，有

$$\varphi(e_1)=(1\ 0\ 0)=e_1$$

$$\varphi(e_2)=(0\ 1\ 0)=e_2$$

$$\varphi(e_3)=(0\ 0\ -1)=-e_3$$

于是有：$[\varphi(e_1)]_U=(1\ 0\ 0)$；$[\varphi(e_2)]_U=(0\ 1\ 0)$；$[\varphi(e_3)]_U=(0\ 0\ -1)$。从而得

$$\mathrm{Mat}_U\varphi=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

关于 K—基 $F=\{f_1=(1\ 0\ 1),\ f_2=(0\ 1\ 0),\ f_3=(0\ 0\ 1)\}$，有

$$\varphi(f_1)=(1\ 0\ -1)=f_1-2f_3$$

$$\varphi(f_2)=(0\ 1\ 0)=f_2$$

$$\varphi(f_3)=(0\ 0\ -1)=-f_3$$

于是有：$[\varphi(f_1)]_F=(1\ 0\ -2)$；$[\varphi(f_2]_F=(0\ 1\ 0)$；$[\varphi(f_3)]_F=(0\ 0\ -1)$，从而得

$$\mathrm{Mat}_F\varphi=\begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

下面再看一下 K—向量空间 V 中，K—基的演化对线性变换阵的影响。

定理 5 设 V 是除环 K 上的向量空间，如果 K—基 X 到

K—基 Y 的演化阵是 C，φ 是 V 上的线性变换且

$$\text{Mat}_X(\varphi)=A,\quad \text{Mat}_Y(\varphi)=B$$

则

$$B=CAC^{-1}$$

此定理的证明作为练习。

例11　在例10中，已知K—向量空间 $K^{(3)}$ 中镜面反射 φ 在 K— 基 U 上的阵为

$$\text{Mat}_U=\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}$$

而K—基 U 到 K—基 F 的演化阵为

$$C=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}$$

于是得

$$\text{Mat}_F(\varphi)=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}\begin{pmatrix}1&0&-1\\0&1&0\\0&0&1\end{pmatrix}$$

$$=\begin{pmatrix}1&0&-2\\0&1&0\\0&0&-1\end{pmatrix}$$

再观察一下 K—向量空间 V 上的线性变换的总体，令

$$\text{End}_K(V)=\{\varphi:\ V\to V\mid\varphi\text{ 是 }V\text{ 上的线性变换}\}$$

（1）$\forall\varphi,\ \psi\in\text{End}_K(V)$，规定“+”为

$$(\varphi+\psi)(x)=\varphi(x)+\psi(x),\quad\forall x\in V$$

则 $\varphi+\psi$ 是 V 上的线性变换，这是因为

（i） $\forall x,\ y\in V$有

$$(\varphi+\psi)(x+y)=\varphi(x+y)+\psi(x+y)$$
$$=\varphi(x)+\varphi(y)+\psi(x)+\psi(y)$$
$$=(\varphi+\psi)(x)+(\varphi+\psi)(y)$$

（ii） $\forall x\in V,\ k\in K$，有

$$(\varphi+\psi)(kx)=\varphi(kx)+\psi(kx)$$
$$=k\varphi(x)+k\psi(x)$$
$$=k(\varphi+\psi)(x)$$

故$\varphi+\psi\in \mathrm{End}_K(V)$，且$\{\mathrm{End}_K(V),\ +\}$是加群，称为$K$—向量空间$V$上的线性变换加群。

（2） 令Δ是除环K的中心子域，$\forall\delta\in\Delta,\ \varphi\in \mathrm{End}_K(V)$，规定"·"为

$$(\delta\cdot\varphi)x=\delta(\varphi(x)),\quad \forall x\in V$$

则$\delta\cdot\varphi$是V上的线性变换，这是因为

（i） $\forall x,\ y\in V$，有

$$(\delta\cdot\varphi)(x+y)=\delta(\varphi(x+y))$$
$$=\delta(\varphi(x)+\varphi(y))$$
$$=\delta(\varphi(x))+\delta(\varphi(y))$$
$$=(\delta\cdot\varphi)(x)+(\delta\cdot\varphi)(y)$$

（ii） $\forall x\in V,\ k\in K$，有

$$(\delta\cdot\varphi)(kx)=\delta(\varphi(kx))=\delta(k\varphi(x))$$
$$=(\delta k)\varphi(x)=(k\delta)\varphi(x)$$
$$=k(\delta(\varphi(x)))=k(\delta\cdot\varphi)(x)$$

故$\delta\cdot\varphi\in \mathrm{End}_K(V)$。在代数运算"·"下，加群$\mathrm{End}_K(V)$构成$\Delta$上的向量空间。

（3） $\forall\varphi,\ \psi\in \mathrm{End}_K(V)$，规定"$\circ$"为

$$(\varphi\circ\psi)(x)=\varphi(\psi(x)),\quad \forall x\in V$$

则$\varphi\circ\psi$是V上的线性变换，这是因为

（i） $\forall x,\ y\in V$，有

$$(\varphi\circ\psi)(x+y)=\varphi[\psi(x+y)]=\varphi(\psi(x))+\varphi(\psi(y))$$
$$=(\varphi\circ\psi)(x)+(\varphi\circ\psi)(y)$$

(ii) $\forall x\in V$，$k\in K$ 有

$$(\varphi\circ\psi)(kx)=\varphi(\psi(kx))=\varphi(k\psi(x))$$
$$=k(\varphi\circ\psi)(x)$$

故 $\varphi\circ\psi\in \mathrm{End}_K(V)$。且易验证 $\{\mathrm{End}_K(V),\ +,\ \circ\}$ 是环，称为K—向量空间 V 上的**线性变换环**。

综合上述可知：K—向量空间 V 上的线性变换集合$\mathrm{End}_K(V)$ 满足，

（1） $\mathrm{End}_K(V)$ 是 K 的中心子域Δ上的向量空间。

（2） $\mathrm{End}_K(V)$ 的乘法运算 "$\circ$" 适合

（a） $\varphi\circ(\psi+\rho)=\varphi\circ\psi+\varphi\circ\rho$

$(\psi+\rho)\circ\varphi=\psi\circ\varphi+\rho\circ\varphi$

（b） $\forall\ \delta\in\Delta$，ϕ，$\psi\in \mathrm{End}_K(V)$ 有

$$(\delta\cdot\varphi)\circ\psi=\varphi\circ(\delta\cdot\psi)=\delta\cdot(\varphi\circ\psi)$$

称满足此条件的代数体系 $\mathrm{End}_K(V)$ 为除环 K 上的**线性变换代数**。

对于除环 K 上的 n 阶矩阵环$M_n(K)$。在 K 上也具有

（1） $M_n(K)$ 是 K 的中心子域Δ上的向量空间。

（2） $M_n(K)$的乘法满足

（a） $\forall A$，B，$C\in M_n(K)$，有

$A(B+C)=AB+AC$

$(B+C)A=BA+CA$

（b） $\forall\delta\in\Delta$，A，$B\in M_n(K)$，有

$(\delta A)B=A(\delta B)=\delta(AB)$

称满足此条件的代数体系$M_n(K)$为除环 K 上的**矩阵代数**。

令$X=\{x_i\}_{i=1}^n$是向量空间 V 的一个K—基。

$$\mathrm{Mat}_X:\ \ \mathrm{End}_K(V)\longrightarrow M_n(K)$$

$$\varphi \longmapsto \mathrm{Mat}_X(\varphi)$$

是 $\mathrm{End}_K(V)$ 到 $M_n(K)$ 的双射，且满足

（1）$\forall\ \varphi,\ \psi \in \mathrm{End}_K(V)$，有

$$\mathrm{Mat}_X(\varphi+\psi)=\mathrm{Mat}_X(\varphi)+\mathrm{Mat}_X(\psi)$$

（2）$\forall\ \varphi \in \mathrm{End}_K(V)$，$\delta \in \Delta$，有

$$\mathrm{Mat}_X(\delta\cdot\varphi)=\delta\mathrm{Mat}_X(\varphi)$$

（3）$\forall\ \varphi,\ \psi \in \mathrm{End}_K(V)$，有

$$\mathrm{Mat}_X(\varphi\circ\psi)=\mathrm{Mat}_X\psi\ \ \mathrm{Mat}_X(\varphi)$$

此时，称 $\mathrm{End}_K(V)$ 与 $M_n(K)$ 是除环 K 上的反同构代数。于是可将 $M_n(K)$ 看作 $\mathrm{End}_K(V)$ 的一个具体表示，一些课题就可以在 $M_n(K)$ 中进行研究了。

习　　题

1　在 K—向量空间 V 中，如果 $x_1,\ x_2,\ \cdots,\ x_m$ 是线性无关的，而 $x_1,\ x_2,\ \cdots,\ x_m,\ x_{m+1}$ 是线性相关的，则 x_{m+1} 可被 $x_1,\ x_2,\ \cdots,\ x_m$ 线性表出。

2　令 $x_1,\ x_2,\ \cdots x_m$，$(m>1)$ 是 K—向量空间 V 的一个向量组，$x_1',\ x_2',\ \cdots,\ x_m'$ 是 V 的另一个向量组，且有

$$x_i'=x_i,\quad i=1,2,\cdots,m-1$$
$$x_m'=x_m+bx_1$$

则 $x_1,\ x_2,\ \cdots,\ x_m$ 是线性相关的，必要而且只要 $x_1',\ x_2'\ \cdots,\ x_m'$ 是线性相关的。

3　令 $x_1,\ x_2,\ \cdots,\ x_m$ $(m>1)$ 是 K—向量空间 V 的一个向量组，且

$$x_1'=x_1$$
$$x_j'=x_j+b_jx_1,\quad j=2,\cdots,m$$

那么 $x_1,\ x_2,\ \cdots,\ x_m$ 是线性无关的，必要而且只要 $x_1',\ x_2',\ \cdots,$

x^{m} 是线性无关的。

4　在除环K上n维向量空间中，$n+1$个向量一定线性相关。

5　在除环K上以$\{e_i\}_{i=1}^{n}$为K—基的n维向量空间中，向量组

$$\left\{ x_i = \sum_{j=1}^{n} a_{ij} e_j \right\}_{i=1}^{m}$$

是线性相关的，必要而且只要线性方程组

$$\begin{aligned} &\xi_1 a_{11} + \xi_2 a_{21} + \cdots + \xi_m a_{m1} = 0 \\ &\xi_1 a_{12} + \xi_2 a_{22} + \cdots + \xi_m a_{m2} = 0 \\ &\cdots \quad \cdots \quad \cdots \quad \cdots \\ &\xi_1 a_{1n} + \xi_2 a_{2n} + \cdots + \xi_m a_{mn} = 0 \end{aligned}$$

有一个非零解：$(\xi_1\ \xi_2\ \cdots\ \xi_m) = (b_1\ b_2\ \cdots b_m)$，$b_i \in K$。

6　对除环K上线性方程组

$$\sum_{i=1}^{m} \xi_i a_{ij} = 0, \quad j=1, 2, \cdots, n$$

如果$m>n$，则在除环K上有非零解。

7　设f_1，f_2，…，f_r是除环K上n维向量空间V的一个线性无关向量组，$U=\{e_i\}_{i=1}^{n}$是V的一个K—基。则在U中可选出 $n-r$ 个向量：e_{i_1}，e_{i_2}，…，$e_{i_{n-r}}$使

$$\{f_1,\ f_2,\ \cdots,\ f_r,\ e_{i_1},\ e_{i_2},\ \cdots,\ e_{i_{n-r}}\}$$

是V的又一个K—基。

8　设K是四元数除环，证明，环模K是向量空间，求出两个不同的K—基及这两个K—基间的演化阵，并对线性变换

$$\varphi:\ a+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k} \longmapsto a-b\boldsymbol{i}-c\boldsymbol{j}-d\boldsymbol{k}$$

求出所得K—基上的阵。

如果将K看作实数域$\boldsymbol{R}$上的向量空间，再找出一个$\boldsymbol{R}$—基，并求出φ的阵。

9　设R是有$1\neq 0$的交换环，R的所有非可逆元构成R的极大理想B，M是R上的有限生成模。此时，商环$\overline{R}=R/B$是除环，证明，

（1）BM是M的子群；

（2）对于商群 $M/BM=\{\overline{x}=x+BM \mid x\in M\}$和商环$R/B=\{\overline{r}=r+B \mid r\in R\}$ 若规定

$$\overline{r}\,\overline{x}=\overline{rx}=rx+BM,\ \forall\ \overline{r}\in R/B,\ \overline{x}\in M/BM$$

则M/BM是$\overline{R}$上的向量空间；

（3）若$U=\{u_i\}_{i=1}^n$是模M的最小生成集，则$\overline{U}=\{\overline{u}_i=u_i+BM\}_{i=1}^n$是$R/B$—向量空间$M/BM$的一个$R/B$—基。

§6 子模和商模

同正规子群和理想的提出一样，在R—模M中提出子模的概念，来考查模M的结构；同商群和商环概念的提出一样，在R—模M中提出商模的概念，对模M的元素进行分类，来建立R—模M的同态象。

定义1　设M是环R上的模，$N\neq\phi$是M的子集，如果按R—模M中的运算，N是环R上的模时，则称N为模M的R—子模．或简称为M的子模．

对于R—模M来说，M和$\{\theta\}$是它的两个当然子模．M的非当然子模N叫做M的**真子模**．

如果R—模M不存在真子模，则称M为R—单模．易证

定理1　设$N\neq\phi$是R—模M的子集，则N是M的子模，必要而且只要

（1）$\forall x,\ y\in N$，有$x-y\in N$；

（2）$\forall x\in N$，$r\in R$，有$rx\in N$．

子模的构造方法之一，是用“生成”这样一种手段．设S是R—模M的一个非空子集，

$$L(S)=\left\{\sum_{i=1}^{n}a_ix_i\,|\,a_i\in R,\ x_i\in S,\ n\in N\right\}$$

是S中元素在R上的所有线性组合的集合，易证

（1）$\forall\ x=\sum_{i=1}^{n}a_ix_i,\ y=\sum_{j=1}^{m}b_jy_j\in L(S)$，有$x-y\in L(S)$；

（2）$\forall\ x=\sum_{i=1}^{t}a_ix_i\in L(S)$，$r\in R$，有$rx\in L(S)$．故

知，$L(S)$ 是R—模M的子模，称为**由子集S生成的子模**。

容易看出：由子集S生成的子模$L(S)$，是M中含子集S的最小子模。如果N是R—模M的一个生成集，且 $N\subseteq S$，则 $L(S)=M$。

例 1　考察Z_6—模$Z_6^{(3)}$

取　$x=(\bar{5}\ \ \bar{0}\ \ \bar{0})$，　$y=(\bar{0}\ \ \bar{2}\ \ \bar{0})\in Z_6^{(3)}$，则有：

$$
\begin{aligned}
L(x)=\{&(\bar{0}\ \bar{0}\ \bar{0}),\ (\bar{5}\ \bar{0}\ \bar{0}),\ (\bar{4}\ \bar{0}\ \bar{0}),\\
&(\bar{3}\ \bar{0}\ \bar{0}),\ (\bar{2}\ \bar{0}\ \bar{0}),\ (\bar{1}\ \bar{0}\ \bar{0})\}\\
L(y)=\{&(\bar{0}\ \bar{0}\ \bar{0}),\ (\bar{0}\ \bar{2}\ \bar{0}),\ (\bar{0}\ \bar{4}\ \bar{0})\}\\
L(x,\ y)=\{&(\bar{0}\ \bar{0}\ \bar{0}),\ (\bar{5}\ \bar{0}\ \bar{0}),\ (\bar{4}\ \bar{0}\ \bar{0}),\\
&(\bar{3}\ \bar{0}\ \bar{0}),\ (\bar{2}\ \bar{0}\ \bar{0}),\ (\bar{1}\ \bar{0}\ \bar{0}),\\
&(\bar{0}\ \bar{2}\ \bar{0}),\ (\bar{5}\ \bar{2}\ \bar{0}),\ (\bar{4}\ \bar{2}\ \bar{0}),\\
&(\bar{3}\ \bar{2}\ \bar{0}),\ (\bar{2}\ \bar{2}\ \bar{0}),\ (\bar{1}\ \bar{2}\ \bar{0}),\\
&(\bar{0}\ \bar{4}\ \bar{0}),\ (\bar{5}\ \bar{4}\ \bar{0}),\ (\bar{4}\ \bar{4}\ \bar{0}),\\
&(\bar{3}\ \bar{4}\ \bar{0}),\ (\bar{2}\ \bar{4}\ \bar{0}),\ (\bar{1}\ \bar{4}\ \bar{0})\}
\end{aligned}
$$

x在Z_6上是自由元，$L(x)$ 是$Z_6^{(3)}$的1秩自由模，y在Z_6上是非自由元，$L(y)$ 是Z_6的非自由的循环子模。

例 2　设K是除环，考查K—向量空间$K^{(n)}$，对于K—基 $U=\{e_i\}_{i=1}^{n}$，其中 $e_i=(\underbrace{0\ 0\ \cdots\ 0\ 1}_{i}\ 0\ \cdots\ 0)\ (i=1,2,\cdots,n)$有

$$
\begin{aligned}
L(\theta)&=\{\theta\}=\{(0\ 0\ \cdots\ 0)\}\\
L(e_1)&=\{k_1e_1\,|\,k_1\in K\}\\
&=\{(k_1\,0\ \cdots\ 0)\,|\,k_1\in K\}\\
L(e_1,\ e_2)&=\{k_1e_1+k_2e_2\,|\,k_1,\ k_2\in K\}\\
&=\{(k_1\ k_2\ 0\ \cdots 0)\,|\,k_1,\ k_2\in K\}
\end{aligned}
$$

在子空间 $L(\theta)=\{\theta\}$ 中，不存在K—基，规定其维数为零；在$L(e_1)$中，$\{e_1\}$是它的一个K—基，它是一维子空间；在$L(e_1,\ e_2)$中，$\{e_1,\ e_2\}$ 是它的一个K—基，它是二维子空间；再看

$$L(e_1+e_2)=\{k(e_1+e_2)\,|\,\forall k\in K\}$$

$$=\{(k\quad k\ 0\cdots 0)\mid k\in K\}$$

它的K—基是 $\{e_1+e_2\}=\{(1\ 1\ 0\ \cdots\ 0)\}$，它是一维子空间，而

$$L(U)=\left\{\sum_{i=1}^{n}k_ie_i\mid k_i\in K\right\}$$
$$=\{(k_1\quad k_2\quad\cdots\quad k_n)\mid k_i\in K,\ i=1,2,\cdots,n\}$$
$$=M$$

通过例1知交换环上自由模，子模不一定是自由的；而通过例2却看到除环上向量空间的子模，则一定是向量空间。

对一般环R来说，由于其理想N具有吸收性，即 RN，$NR\subseteq N$，由此启示我们一个构造子模的新途径

设M是环R上的模，N是R的左理想，令

$$NM=\left\{\sum_{i=1}^{n}a_ix_i\mid a_i\in N,\ x_i\in M,\ \forall n\in N\right\}$$

是M元素在N上的线性组合的集合．它是M的子集，且有

（1）若$x=\sum_{i=1}^{n}a_ix_i$，$y=\sum_{i=1}^{m}b_iy_i\in NM$，则

$$x-y=\sum_{i=1}^{n}a_ix_i-\sum_{i=1}^{m}b_iy_i=\sum_{i=1}^{n+m}c_kz_k\in NM.$$

其中

$$c_kz_k=\begin{cases}a_ix_i & \text{当}k=i\text{时}\\ -b_iy_i & \text{当}k=n+i\text{时}\end{cases}$$

（2）若 $k\in R$，$x=\sum_{i=1}^{n}a_ix_i\in NM$，则

$$kx=\sum_{i=1}^{n}(ka_i)x_i\in NM$$

这是由于N是R的左理想，$RN\subseteq N$．于是对于$\forall a_i\in N$，$k\in R$，都有 $ka_i\in N$。从而断定 $kx\in NM$．由（1）和（2）可知：NM是M的R—子模．

例3　考查环模$M_2(Z)$，则

$$N=\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\in M_2(\mathbf{Z})\,\middle|\, a,\ b\in \mathbf{Z}\right\}$$

是环$M_2(\mathbf{Z})$的左理想。$\forall\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\in N$，$\begin{pmatrix} x & y \\ z & u \end{pmatrix}\in M_2(\mathbf{Z})$，有

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & u \end{pmatrix}=\begin{pmatrix} ax & ay \\ bx & by \end{pmatrix}=\begin{pmatrix} a \\ b \end{pmatrix}(x \quad y)$$

于是模$M_2(\mathbf{Z})$的子模

$$NM_2(\mathbf{Z})=\left\{\sum_{i=1}^{n}\begin{pmatrix} a_i \\ b_i \end{pmatrix}(x_i, y_i)\,\middle|\, a_i, b_i, x_i, y_i\in \mathbf{Z},\ \forall n\in N\right\}$$

例 4　考查环模：$\mathbf{Z}_6$，则

$$N=\{\bar{0},\ \bar{2},\ \bar{4}\}$$

是环$\mathbf{Z}_6$的标量$\bar{2}$所生成的理想。于是模$\mathbf{Z}_6$的子模

$$N\mathbf{Z}_6=\{\bar{0},\ \bar{2},\ \bar{4}\}.$$

例 5　考查$\mathbf{Z}$—模 $\mathbf{Z}^{(3)}$

$$N=(3)=\{k3\mid k\in \mathbf{Z}\}$$

是环$\mathbf{Z}$中，标量 3 所生成的理想，于是模$\mathbf{Z}^{(3)}$有子模

$$N\mathbf{Z}^{(3)}=\{(a_1 \quad a_2 \quad a_3)\mid a_i\in N,\ i=1,2,3\}=N^{(3)}.$$

下面看一下子模的合成。

设N_1和N_2是R—模M的两个子模，则N_1与N_2的交

$$N_1\cap N_2=\{x\in M\mid x\in N_1,\ x\in N_2\}\neq\phi$$

而且 $N_1\cap N_2$ 是M的子模。事实上，

（1）若 x，$y\in N_1\cap N_2$ 则 x，$y\in N_1$；x，$y\in N_2$。故有$x-y\in N_1$，$x-y\in N_2$。所以 $x-y\in N_1\cap N_2$。

（2）若 $x\in N_1\cap N_2$，$k\in R$，则 $x\in N_1$，$x\in N_2$。故有$kx\in N_1$，$kx\in N_2$，所以$kx\in N_1\cap N_2$。故$N_1\cap N_2$是模M的子模。

令

$$N_1+N_2=\{x_1+x_2 \mid x_1\in N_1,\ x_2\in N_2\}$$

于是有

（1）若 $x,\ y\in N_1+N_2$ 则 $x=x_1+x_2,\ y=y_1+y_2,\ x_1,\ y_1\in N_1;\ x_2,\ y_2\in N_2$。故有$x_1-y_1\in N_1, x_2-y_2\in N_2$，从而得

$$x-y=(x_1+x_2)-(y_1+y_2)$$
$$=(x_1-y_1)+(x_2-y_2)\in N_1+N_2$$

（2）若 $x=x_1+x_2\in N_1+N_2$。$x_1\in N_1,\ x_2\in N_2;\ k\in R$，则$kx_1\in N_1\ \ kx_2\in N_2$从而得

$$kx=k(x_1+x_2)=kx_1+kx_2\in N_1+N_2$$

所以N_1+N_2是模M的子模，称此子模为N_1与N_2的和．特别是，对 N_1+N_2 来说，如果有

$$x_1+x_2=\theta \Longleftrightarrow x_1=\theta,\ x_2=\theta$$

则称和 N_1+N_2 为直和，记作$N_1\oplus N_2$。

当然，子模的交与和可推广到多个子模的合成上。

例 6 设M是环R上的n秩自由模，$U=\{u_i\}_{i=1}^n$ 是M的R—自由基．则对1秩子模Ru_i来说，定有$n-1$秩自由子模H存在，使

$$M=Ru_i\oplus H$$

解 不妨取$i=1$，则$H=L(u_2,\ \cdots,\ u_n)$即为所求。

和其他代数体系一样，给了子代数体系，就可以将原代数体系进行分类，得到商集，进而在商集上去窥测原代数体系的一些性质。

设N是R—模M的子模，则N关于加群M的加法运算构成M的子群．用N作M的商集

$$M/N=\{x+N \mid x\in M\}$$

这是模元素用子模N作分类而得的商集，在M/N中，对 $x+N$ 和 $y+N$，如果规定

$$(x+N)+(y+N)=(x+y)+N$$

则M/N构成加群（这就是加群M关于子群N所作的商群）．$\forall\ x+N\in M/N,\ k\in R$，如果规定

$$k(x+N)=kx+N$$

则加群 M/N 构成 R 上的模。称 R—模 M/N 为M关于子模N的R—商模，或简称为子模N的商模。

例 7　设M是环 R 上的 n 秩自由模，$U=\{u_i\}_{i=1}^{n}$ 是M的 R—自由基。于是

$$N=L(u_1,u_2,\cdots,u_m)\quad\left\{\sum_{i=1}^{m}a_iu_i\,|\,a_i\in R,\ m<n\right\}$$

是M的m秩自由子模。那么子模N的商模M/N是$n-m$秩自由模。

解　由于

$$\begin{aligned}M/N&=\{x+N\,|\,x\in M\}\\&=\left\{\sum_{i=1}^{n}a_iu_i+N\,|\,a_i\in R\right\}\\&=\left\{\sum_{i=1}^{n}a_i(u_i+N)\,|\,a_i\in R\right\}\\&=\left\{\sum_{i=m+1}^{n}a_i(u_i+N)a_i\in R\right\}\quad(\because u_i\in N,\ 1\leq i\leq m)\end{aligned}$$

于是可知$\overline{U}=\{u_i+N\}_{i=m+1}^{n}$是$M/N$在$R$上的一个生成集；又，如果

$$\sum_{i=m+1}^{n}k_i(u_i+N)=\overline{0}$$

则 $\sum\limits_{i=m+1}^{n}k_iu_i\in N$，于是有

$$\sum_{i=m+1}^{n}k_iu_i=\sum_{i=1}^{m}b_iu_i$$

由U是自由基，可断定$k_i=0$，$i=m+1,m+2,\cdots,n$。从而知$\overline{U}$是 M/N 在R上的自由基，R—模M/N是$n-m$秩自由模。

例 8　考查Z—模$Z^{(2)}$，令$N=(2)$是Z的以 2 生成的理想，于是得到M的子模

$$NZ^{(2)}=\{(a_1,a_2)\in Z^{(2)}\,|\,a_i\in N,\ i=1,2\}=N^{(2)}$$

模 $\mathbf{Z}^{(2)}$关于子模 $N\mathbf{Z}^{(2)}$的商模

$$\begin{aligned}\mathbf{Z}^{(2)}/N\mathbf{Z}^{(2)} &= \{(x_1,x_2)+N^{(2)} \mid (x_1,x_2)\in \mathbf{Z}^{(2)}\}\\ &= \{(x_1+N,x_2+N) \mid x_1,x_2\in \mathbf{Z}\}\\ &\cong \mathbf{Z}_2^{(2)}\end{aligned}$$

于是知：$\mathbf{Z}^{(2)}/N\mathbf{Z}^{(2)}$在$\mathbf{Z}$上不再是自由的了，由此两例知自由模的商模不一定是自由模。

习　　题

1　证明：除环K上n维向量空间中，1维K—子空间是单模。并举例说明，对环R上的n秩自由模来说，相应结论不一定成立。

2　证明：除环K上n维向量空间中，二不同的1维子空间，交点不能多于1个。举例说明，对环R上n秩自由模来说，相应结论不一定成立。

3　设环R上模M（不要求是单式的）是单模，证明：当$RM=\theta$时，M只含p个模向量（p为素数）；当$M=Rx$是循环模时，M中任一非零向量都可以作生成元。

4　在R—模M中，B是R的一个右理想，则M的子集

$N=\{x\in M \mid bx=\theta,\forall\ b\in B\}$

是M的子模。

5　设C是环R的中心，M是R上的模，证明

$N=\{x\in M \mid ax=\theta\ \ a\in C\}$

是M的子模，称为a的零化子模。

$B=\{a\in R \mid ax=\theta,\ x\in M\}$

是R的左理想，称为x的左零化理想。简称x在R里的左零化子。也叫x在R里的阶理想。

6　设K是除环，V是K上n维左向量空间，S是V的m维子空间，证明：商模V/S是$n-m$维K—向量空间。

7　设V是K上n维左向量空间。S_1是m_1维子空间，S_2是m_2维子空间，证明

(S_1+S_2)的维数$=m_1+m_2-(S_1\cap S_2)$的维数

8　设S_1和S_2是R—模M的两个子模，则$S_1\cap S_2=\theta$必要而且只要$S_1+S_2=S_1\oplus S_2$。

9　设x和y是除环K上左向量空间的两个非零向量，如果

$$L(x)+L(y)=L(x)\oplus L(y)$$

则x，y一定是线性无关的。举例说明，在一般环R上的模中，结论不一定成立。

10　对于环模$\mathbf{Z}$，设P是素数，k为正整数，则

$$N=\{np^k \mid \forall n\in \mathbf{Z}\}$$

是模$\mathbf{Z}$的子模。证明：商模$\mathbf{Z}/N$不能表成两个真子模的直和。

11　设R是有$1\neq 0$的交换环，且所有非可逆元皆含于一个真理想B中，则对R上的有限生成模M来说，有

（1）如果A是R的真理想，且$AM=M$，则$M=\{\theta\}$。

（2）如果A是R的真理想，N是模M的子模，且有$M=AM+N$，则$M=N$。

§7　态　射

模是环和加群在倍乘运算下所成的代数体系，所以在研究两个模之间的映射时，既要考虑到加群部分的对应关系，也要考虑到环之间的联系。因此要通过稍为复杂的映射概念—“态射”，来刻画两个模之间的联系。

§4中，在R—自由模M上，提出了R—自同态的概念。自由模M的R—自同态φ是加群M的自同态，且对φ下所含R中的标量因子r可以完整不变的析到φ的外边来。即

（1）$\varphi(x+y)=\varphi(x)+\varphi(y)$

（2）$\varphi(rx)=r\varphi(x)$

$\forall x$，$y\in M$，$r\in R$都成立。

§5中，对除环K上向量空间V，提出了线性变换的概念。向量空间V上的线性变换φ是加群V的自同态，且对φ下K中的标量因子k，可以完整不变的析到φ的外边来，即

（1）$\varphi(x+y)=\varphi(x)+\varphi(y)$

（2）$\varphi(kx)=k\varphi(x)$

$\forall x$，$y\in V$，$k\in K$都成立。

将这两种映射规则推广到一般的环 R，对于 R—模 M。给出

定义 1　设 φ 是 R—模 M 上的一个变换，如果满足

（1） $\varphi(x+y)=\varphi(x)+\varphi(y)$

（2） $\varphi(rx)=r\varphi(x)$

$\forall x,\ y\in M,\ r\in R$。则称 φ 为模 M 上的 R—自同态，特别 φ 是双射时，叫做模 M 的 R—自同构。

对模 M 上的 R—自同态 φ 来说，称 M 的子集

$$\ker\varphi=\{x\in M\mid\varphi(x)=\theta\}$$

为 φ 的核。显然 φ 的核是 M 的子模。

显然 φ 的象

$$\operatorname{im}(\varphi)=\{y\in M\mid y=\varphi(x),\ \ \forall x\in M\}$$

也是 M 的子模。

模 M 的 R—自同态，是 R—模 M 自身的一种变换。

对环 R 上的两个模 M_1 和 M_2 来说，可进一步将 R—自同态的规则推广到模 M_1 和模 M_2 间的映射上。这时将有

定义 2　设 R 是环，M_1 和 M_2 是两个 R—模，如果 φ：$M_1\to M_2$ 满足

（1） $\varphi(x+y)=\varphi(x)+\varphi(y)$

（2） $\varphi(rx)=r\varphi(x)$

$\forall x,\ y\in M,\ r\in R$。则称 φ 为模 M_1 到模 M_2 的 R—同态。当 φ 是满射时，则说模 M_1 和模 M_2 是 R—同态的，记作 $M_1\overset{\varphi}{\sim}M_2$；当 φ 是双射时，则说模 M_1 和模 M_2 在 φ 下是 R—同构的，记作 $M_1\overset{\varphi}{\cong}M_2$。

例 1　设 φ 是模 M 的 R—自同态，子模 $\ker\varphi$ 对 M 的商模 $M/\ker\varphi$ 仍是环 R 上的模、考察 R 上的模 $\operatorname{im}\varphi$ 和模 $M/\ker\varphi$。令

$$\overline{\varphi}:\ \operatorname{im}(\varphi)\longrightarrow M/\ker\varphi$$
$$y\longmapsto x+\ker\varphi$$

$\forall\ y=\varphi(x)\in\operatorname{im}\varphi$，则 $\overline{\varphi}$ 是模 $\operatorname{im}\varphi$ 到模 $M/\ker\varphi$ 的 R—同构。

解 令 $y_1=\varphi(x_1)$，$y_2=\varphi(x_2)\in \text{im}\varphi$，如果 $\overline{\varphi}(y_1)=\overline{\varphi}(y_2)$ 则有 $x_1+\ker\varphi=x_2+\ker\varphi$，于是 $x_1-x_2\in\ker\varphi$，从而得

$$\theta=\varphi(x_1-x_2)=\varphi(x_1)-\varphi(x_2)=y_1-y_2$$

故知 $\overline{\varphi}$ 是单射．又因，$\forall x+\ker\varphi\in M/\ker\varphi$，有

$\varphi(x)=y\in \text{im}\varphi$，于是 $\overline{\varphi}(y)=x+\ker\varphi$，故知 $\overline{\varphi}$ 是满射，且有

$$\begin{aligned}(1)\quad \overline{\varphi}(y_1+y_2)&=(x_1+x_2)+\ker\varphi\\&=(x_1+\ker\varphi)+(x_2+\ker\varphi)\\&=\overline{\varphi}(y_1)+\overline{\varphi}(y_2)\end{aligned}$$

$$\begin{aligned}(2)\quad \overline{\varphi}(ry_1)&=rx_1+\ker\varphi=r(x_1+\ker\varphi)\\&=r\overline{\varphi}(y_1)\end{aligned}$$

$\forall y_1$，$y_2\in \text{im}\varphi$，$r\in R$ 都成立，于是得

$$\text{im}\varphi\overset{\overline{\varphi}}{\cong}M/\ker\varphi$$

对于环 R 上的模 M_1 和模 M_2，如果 φ 是 M_1 到 M_2 的 R—同态，则称 M_1 的子集

$$\ker\varphi=\{x\in M_1\,|\,\varphi(x)=\theta\in M_2\}$$

为 φ 的核，显然 φ 的核是 M_1 的子模．称 M_2 的子集

$$\text{im}\varphi=\{y\in M_2\,|\,y=\varphi(x),\ \ \forall x\in M_1\}$$

为 φ 的象．显然 φ 的象是 M_2 的子模．且 M_1 与 $\text{im}\varphi$ 在映射 φ 下是满同态的．即 $M_1\overset{\varphi}{\sim}\text{im}\varphi$．

同态基本定理 设 H 是 R—模 M 的子模，则

（1）存在模 M 到商模 M/H 的 R—满同态 φ，且 $\ker\varphi=H$；

（2）若 R—模 M 和 R—模 M' 是 R—满同态的，同态核是 H，则 M' 与 M/H 是 R—同构的．

这一定理的证明，可仿群的同态基本定理去作．

例 2　设 R 是有 $1\neq0$ 的环，$M=Rx$ 是 x 在 R 上生成的循环模．令

$$\begin{aligned}\varphi:\ &R\longrightarrow M=Rx\\&r\longmapsto rx\in M,\ \ \forall\ r\in R\end{aligned}$$

则 φ 是环模 R 到 R—循环模 M 的 R—同态，且有

$$\mathrm{im}\varphi = Rx,\quad \ker\varphi = \{r\in R \mid rx=\theta\}$$

此时，$\ker\varphi$ 是环的理想，称为 x 在 R 里的零化子,记作 $\mathrm{ann}x$，于是有

$$R/\mathrm{ann}x \cong Rx$$

当 $R=Z$ 时，对 Z—循环模 Zx 来说，x 在 Z 里的零化子

$$\mathrm{ann}x=\ker(\varphi)=(n)$$

是非负整数 n 在 Z 中生成的理想。n 是使 $nx=\theta$ 成立的最小正整数，是模元素 x 的阶。所以对一般的 R—模 M 来说，$x\in M$，x 在 R 里的零化子 $\mathrm{ann}x$ 叫作 x 在 R 里的阶理想。

R 上同构的模是具有共同代数性质的模，是在代数意义下相等的模。因此如何判断两个模是否 R—同构是模论中基本问题之一。对于交换环上自由模和除环上的向量空间，我们有

定理 1 设 M_1 和 M_2 是有 $1\neq 0$ 的交换环 R 上的自由模，那么 $M_1 \overset{\varphi}{\cong} M_2$，必要且只要 M_1 的秩等于 M_2 的秩。

定理 2 设 V_1 和 V_2 是除环 K 上的两个向量空间，那么 $V^1 \overset{\varphi}{\cong} V_2$，必要且只要 V_1 的维数等于 V_2 的维数。

这两个定理的证明，都可以仿照“高等代数”中有关定理加以证明。

例 3 设 M 是环 R 上的 n 秩自由模，$U=\{u_i\}_{i=1}^n$ 是 M 的 R—自由基。对 R—自由模 $R^{(n)}$，令

$$\eta:\ x\longmapsto [x]_U\in R^{(n)},\quad \forall\ x\in M$$

则有

$$M\overset{\eta}{\cong} R^{(n)}$$

从而知：M 的秩数 $=R^{(n)}$ 的秩数。

例 4 设 V 是除环 K 上的 n 维向量空间，那么 V K—同构于 K 上向量空间 $K^{(n)}$。

解 在 $K^{(n)}$ 中取子集

$$E = \{e_i = (\overbrace{0 \cdots 0\ 1\ 0 \cdots 0}^{i})\}_{i=1}^{n}$$

可验证E是$K^{(n)}$的一个K—基，E中含有n个向量，于是知$K^{(n)}$的维数为n，等于V在K上的维数，从而得 $V \cong K^{(n)}$。

在代数意义下，交换环R上的自由模由秩数n所唯一确定，于是$R^{(n)}$就成了R上n秩自由模的典型代表。是研究R上n秩自由模的具体对象；除环K上向量空间由维数n所唯一确定，因而$K^{(n)}$就成了K上n维向量空间的典型代表，是研究K上n维向量空间的具体对象。

在模的进一步研究中，也常提到R—"半同态映射"，它是R—同态映射的自然扩充。

定义 3 设M_1和M_2是环R上的两个模。σ是环R的自同构。如果映射φ：$M_1 \to M_2$满足

（1）$\varphi(x+y) = \varphi(x) + \varphi(y)$

（2）$\varphi(rx) = \sigma(r)\varphi(x)$

$\forall x, y \in M_1, r \in R$都成立，则称$\varphi$为$R$上模$M_1$到$M_2$的关于$\sigma$的半同态，简称作关于$\sigma$的$R$—半同态。特别当$M_1 = M_2 = M$时，则称$\varphi$为$R$上模$M$关于$\sigma$的半自同态。也叫做关于$\sigma$的半线性变换。尤其是当$\varphi$是双射时，则称$\varphi$为关于$\sigma$的$R$—半（自）同构。

例 5 设$R = Z[i] = \{a + bi | a, b \in Z\}$，令

$$\sigma: \alpha = a + bi \longmapsto \overline{\alpha} = a - bi$$

$\forall\ \alpha \in R$，是环R的一个对合自同构，在R上作n秩自由模

$$R^{(n)} = \{(c_1\ \ c_2\ \ \cdots\ \ c_n) | c_i \in R,\ 1 \leq i \leq n\}$$

再令

$$\varphi: R^{(n)} \longrightarrow R^{(n)},\ (c_1\ c_2\ \cdots\ c_n) \longmapsto (\overline{c_1}\ \overline{c_2} \cdots \overline{c_n})$$

则φ是模$R^{(n)}$的关于σ的R—半自同构。

解 φ是$R^{(n)}$上的双射是易知的，而且

（1）当$x = (x_1\ x_2\ \cdots x_n)$、$y = (y_1\ y_2\ \cdots y_n) \in R^{(n)}$时，记$\overline{x} = (\overline{x_1}\ \overline{x_2} \cdots \overline{x_n})$，$\overline{y} = (\overline{y_1}\ \overline{y_2} \cdots \overline{y_n})$，于是有

$$\varphi(x+y) = \overline{x+y} = \overline{x} + \overline{y} = \varphi(x) + \varphi(y)$$

$$\varphi(rx)=\overline{rx}=\overline{r}\ \overline{x}=\overline{r}\varphi(x)=\sigma(r)\varphi(x)$$

从而知φ是$R^{(n)}$上关于σ的R—半自同构。

有了模M的关于σ的R—半同态概念后，可以看到模M的R—同态φ，是M的R—半同态的特例，是关于R恒等自同构的R—半同态。

在对两个环上的模进行比较和建立联系时，常要用到态射这一概念。它是半同态概念的推广。

定义 4 设M是环R上的模，M_1是环R_1上的模，σ是环R到环R_1的同态映射。如果映射φ：$M\to M_1$满足

（1）$\varphi(x+y)=\varphi(x)+\varphi(y)$

（2）$\varphi(rx)=\sigma(r)\varphi(x)$

$\forall x, y\in M, r\in R$。则称$\varphi$是$R$—模$M$到$R_1$—模$M_1$的关于$\sigma$的态射。简记为$\sigma$—态射$\varphi$。

σ—态射φ是一个比关于σ的R—半同态更加广泛的概念。当$R=R_1$时，φ是R—半同态；当$R=R_1$，σ是R上的恒等自同构时，φ是R—同态。

例 6 设M是环R上的n秩自由模。$U=\{u_i\}_{i=1}^{n}$是M的R—自由基。B是环R的理想，$\overline{R}=R/B$是R关于理想B的商环，于是可在$\overline{R}$上作n秩自由模$\overline{R}^{(n)}$。令映射

$$\sigma:\ R\longrightarrow\overline{R}$$
$$r\longmapsto\overline{r}=r+B\in\overline{R},\ \forall r\in R$$

则σ是环R到$\overline{R}$的同态映射。再令

$$\varphi:\ M\longrightarrow\overline{R}^{(n)}$$
$$x=\sum_{i=1}^{n}a_iu_i\longmapsto(\overline{a_1}\ \overline{a_2}\cdots\overline{a_n})\in\overline{R},\quad\forall\quad x\in M$$

则φ是R—模M到$\overline{R}$—模$\overline{R}^{(n)}$的σ—态射。

解 φ是M到$\overline{R}^{(n)}$的映射是易知的，且有

（1）$\forall x=\sum_{i=1}^{n}a_iu_i$、$y=\sum_{i=1}^{n}b_iu_i\in M$，则有

$$x+y=\sum_{i=1}^{n}(a_i+b_i)u_i$$

于是

$$\begin{aligned}\varphi(x+y)&=(\overline{a_1+b_1}\ \ \overline{a_2+b_2}\ \cdots\ \overline{a_n+b_n})\\&=(\overline{a_1}\ \overline{a_2}\cdots\overline{a_n})+(\overline{b_1}\ \overline{b_2}\cdots\overline{b_n})\\&=\varphi(x)+\varphi(y)\end{aligned}$$

（2） $\forall x=\sum_{i=1}^{n}a_iu_i\in M$，$r\in R$，则有

$$rx=\sum_{i=1}^{n}(ra_i)u_i$$

于是

$$\begin{aligned}\varphi(rx)&=(\overline{ra_1}\ \ \overline{ra_2}\ \cdots\ \overline{ra_n})\\&=(\overline{r}\ \overline{a_1}\ \ \overline{r}\ \overline{a_2}\ \cdots\ \overline{r}\ \overline{a_n})\\&=\overline{r}\ (\overline{a_1}\ \ \overline{a_2}\ \cdots\ \overline{a_n})\\&=\sigma(r)\varphi(x)\end{aligned}$$

所以，φ 是 R—模M到$\overline{R}$—模 $\overline{R}^{(n)}$的 σ—态射。

如果φ是满射，则说R—模M与R_1—模M_1在φ下是σ—**同态的**；如果φ是双射，则说R—模M与R_1—模M_1，在φ下是**σ—同构的**。

习　　题

1　设R是有$1\neq 0$的环，M是环R的加法群。定出 R—模M的所有R—自同态，并证明：

$\mathrm{End}_R(M)\cong R$（环同构）

2　令η是R—模M到R—模M'的R—满同态。M的子模$H\supset \ker(\eta)$，$H'=\eta(H)=\{h'=\eta(h)\mid h\in H\}$是$M'$的子模。证明：商模$M/H$与$M'/H'$是$R$—同构的。

3　设φ是R—模M上的关于σ的R—半自同态。证明：

（1）$\varphi((a+b)x)=(\sigma(a)+\sigma(b))\varphi(x)$

（2）$\varphi((ab)x)=\sigma(a)\sigma(b))\varphi(x)$

（3）$\varphi(\sigma^{-1}(a)x)=a\varphi(x)$

4 设M是环R上的n秩自由模，$U=\{u_i\}_{i=1}^n$是M的R—自由基，φ是M上的关于σ的R—半自同态。且有 $\varphi(u_i)=\sum_{j=1}^{n} a_{ij}u_j$，对于$x\in M$，如果$[x]_U=(b_1, b_2, \cdots, b_n)$，$[x]_U^\sigma=(\sigma(b_1), \sigma(b_2), \cdots, \sigma(b_n))$证明，$[\varphi(x)]_U=[x]_U^\sigma A$，其中$A=(a_{ij})$称为$\sigma$—半自同态$\varphi$在$R$—自由基$U$上的阵，记为 $\mathrm{Mat}_U(\varphi)$。

5 对于环R上n秩自由模M，已知σ—半线性变换φ，在R—自由基$U=\{u_i\}_{i=1}^n$上的阵为$A=(a_{ij})$，而M的R—自由基$V=\{v_i\}_{i=1}^n$是U通过可逆阵 $C=(c_{ij})$ 演化而来的，试求φ在V上的阵。

6 对于环R上n秩自由模M，证明，

（1）σ—半线性变换φ与τ—半线性变换ψ之积$\varphi\psi$，仍然是M上的半线性变换。

（2）在M的自由基 $U=\{u_i\}_{i=1}^n$上，如果

$$\mathrm{Mat}_U(\varphi)=A=(a_{ij}),\quad \mathrm{Mat}_U(\psi)=B=(b_{ij})$$

则

$$\mathrm{Mat}_U(\varphi\psi)=B^\sigma A$$

其中 $B^\sigma=(\sigma(b_{ij}))$ 。

7 设R是有$1\neq 0$的交换环，R中非可逆元构成极大理想B。M是R上有限生成模。$\overline{M}=M/BM$是除环$\overline{R}=R/B$上的向量空间，证明，

（1）M的子集 $U=\{u_i\}_{i=1}^n$是M在R上的有限生成集必要且只要$\overline{U}=\{\overline{u_i}=u_i+BM\}_{i=1}^n$是$\overline{R}$上向量空间$\overline{M}$的生成集。

（2）M的子集 $U=\{u_i\}_{i=1}^n$ 是M在R上的最小生成集必要且只要$\overline{U}=\{\overline{u_i}=u_i+BM\}_{i=1}^n$是$\overline{R}$上的向量空间$\overline{M}$的$\overline{R}$—基。

（3）M在R上的两个最小生成集，含有相同多个模元素。

第五章　扩　　域

第三章已给出域的基本概念，本章将进一步讨论域的构造。我们马上会看到，任何一个域都包含着一个结构清楚的所谓素域，而且每个域都可以看做是它的子域的扩张。所以研究域的各种各样的扩张就成为域论的主要内容。限于篇幅，本章只讨论域的几种最基本的扩张。

§1　特征数　素域

特征数和素域是域论中的两个基本概念，特征数是反映一个域的结构的重要标志，我们先证明

定理1　设$\{F;+,\cdot\}$是一个域，则：（1）在加法群$\{F;+\}$中，每个非零元素的阶都相等；（2）如果$\{F;+\}$中非零元素的阶p为有限时，那么p必是素数。

证明（1）$\forall a,b\in F$，$a\neq 0$，$b\neq 0$，取任一非负整数n，则有

$$(na)b=a(nb)$$

于是

$$na=0\Longleftrightarrow nb=0$$

这说明a与b在$\{F;+\}$中的阶相等。

（2）显然$p>1$。假设p不是素数，那么必有$1<p_1$，$p_2<p$使

$$p=p_1p_2$$

于是对于F中的非零元素a有

$$pa=(p_1p_2)a=p_1(p_2a)=0$$

当$p_2a=0$，与p是a的阶相矛盾；当$p_2a\neq 0$，上式表明p_2a的阶不等于p，与本命题中的（1）相矛盾。因此p是素数。证完。

定义1 设$\{F;+,\cdot\}$是一个域，加法群$\{F;+\}$中非零元素的阶叫做域F的特征数。

下面来讨论域的特征数的性质。由定理1知，域F的特征数必是∞或者是素数p，而且还有

推论1 （1）域F的特征数为∞必要而且只要某个$a\in F$，$a\neq 0$和$\forall n\in N$，有$na\neq 0$；（2）域F的特征数为素数p必要而且只要对于某一个非零元素$a\in F$，p是使$pa=0$的最小正整数。

例1 每个数域的特征数都是∞。Z_p（p为素数）的特征数为p。

推论2 设F是域E的子域，则F和E的特征数相同。

事实上，因F和E具有相同的零元和1，由命1题可直接推得。

推论3 n元有限域的特征数必为素数p，而且$p|n$。

命题 设域F的特征数为p，则$\forall a,b\in F$有

$$(a+b)^p=a^p+b^p$$

事实上

$$(a+b)^p=a^p+C_p^1a^{p-1}b+\cdots+C_p^ka^{p-k}b^k+\cdots+b^p$$
$$=a^p+b^p$$

由此命题容易看出，

$$(a+b)^{p^m}=a^{p^m}+b^{p^m}$$

下面来介绍域论的另一个基本概念。

定义2 没有真子域的域叫做素域。

例2 有理数域Q是素域。以素数p为模的剩余类环Z_p是素域。

事实上，设F是Q的子域，显然$1\in F$，而且$\forall n\in Z$有$n(1)=n\in F$。于是$\forall \frac{n}{m}\in Q$，n，m是整数，有n. $m\in F$，从而

$$\frac{n}{m}=n\cdot m^{-1}\in F$$

即$F=Q$。这说明Q没有真子域，即Q是素域。

设E是$\mathbf{Z}_p$的子域，显然$\overline{1}\in E$，于是$\forall\ \overline{n}\in\mathbf{Z}_p$有

$$\overline{n}=n(\overline{1})\in E$$

故$E=\mathbf{Z}_p$。这说明$\mathbf{Z}_p$无真子域，即$\mathbf{Z}_p$是素域。

值得注意的是，从同构角度看，只有这两种类型的素域。

定理 2 设F是任一素域。（1）当F的特征数为∞时，则$F\cong Q$；（2）当F的特征数为p时，则$F\cong\mathbf{Z}_p$。

证明 设e是F的单位元，考虑F的子集

$$S=\{ke\mid k\in\mathbf{Z}\}$$

易证S是F的子环，而且是整环。现将整数环$\mathbf{Z}$与S做比较，令

$$\varphi: n1\longmapsto ne,\quad \forall n\in\mathbf{Z}$$

显然φ是$\mathbf{Z}$到S的满射，并且$\forall n,m\in\mathbf{Z}$有

$$\varphi(n+m)=(n+m)e=ne+me=\varphi(n)+\varphi(m)$$

$$\varphi(nm)=(nm)e=ne\cdot me=\varphi(n)\varphi(m)$$

于是

$$\varphi:\mathbf{Z}\sim S$$

因为φ的核$N=\varphi^{-1}(0)=\{n\in\mathbf{Z}\mid ne=0\}$是$\mathbf{Z}$的一个理想，而$\mathbf{Z}$是主理想环，从而$N$是主理想：$N=(d)$，$d\geqslant 0$。

（1）当F的特征数为∞时，此时$\forall n\in\mathbf{Z}$，$n\neq 0$有$ne\neq 0$，这表明$N=(0)$，所以

$$\varphi:\mathbf{Z}\cong S$$

进而$\mathbf{Z}$的商域Q必与S的商域同构。由于F是素域，所以S的商域恰好是F，因此

$$Q\cong F$$

（2）当F的特征数为p时，这时p是使$pe=0$的最小正整数，即p是$N=(d)$中的最小正整数，从而$p=d$，即$N=(p)$。

由环同态基定理知

$$Z/N \cong S$$

但 $Z/N = Z/(p) = Z_p$ 是域，所以 S 是域。由于 F 是素域，故 $S = F$，从而

$$Z_p \cong F$$

证完。

由于有理数域和以 p 为模的剩余类环都是具体的域，所以定理 2 表明，素域的代数结构是清楚的。一个素域 F，对其代数结构起决定性作用的是它的特征数：当 F 的特征数为 ∞ 时，F 便可看做是有理数域 Q；当 F 的特征数为 p 时，F 便可看做是以 p 为模的剩余类环。

定理 3 任一域 E 必含有唯一的素域。

证明 设 F 是 E 的所有子域的交。显然 F 是 E 的子域。

下面进一步证明，F 是素域。设 F' 是 F 的子域：$F' \subseteq F$，于是 F' 是 E 的子域。由于 F 是 E 的所有子域的交，所以 $F \subseteq F'$ 故 $F' = F$。这说明 F 是素域，即任一域 E 都一定含有是素域的子域。

其次证明，E 所含的素域是唯一的。假设 F_1 也是含在 E 中的素域，则 $F \cap F_1$ 既是 F 的也是 F_1 的子域，但 F 和 F_1 都没有真子域，故

$$F = F \cap F_1 = F_1$$

这说明 E 所含的素域是唯一的。证完。

定义 3 设 F 是域 E 的子域，则 E 叫做 F 的扩张(扩域)，记为 E/F。

显然，任一域 E 都是它所含素域的扩张。从同构观点看，特征数为 ∞ 的域可以看做为有理数域 Q 的扩张，特征数为 p 的域可以看做是以 p 为模的剩余类环 Z_p 的扩张。

习　　题

1　证明，在特征数为 p 有的有限域 E 中，映射 $a \longmapsto a^p$，$\forall a \in E$，是 E 的一个自同构。

2　设E是恰含有四个元素的域，证明，

（1）E的特征数为2；

（2）E中不在素域$\mathbf{Z}_2$中的两个元素都满足

$$x^2=x+1$$

3　设F是特征数为p的域，如果F中的元素都满足方程

$$x^p-x=0$$

则

$$F\cong\mathbf{Z}_p$$

4　试举出一个特征数为P的无限域的例子。

5　找出$\mathbf{Z}_2$上一切三次不可约多项式。

§2　扩　　张

本节对域的扩张做一般性的讨论。

定义1　设E是一个域，F是E的子域，S是E的子集合，则E的所有既包含F又包含S的子域的交叫做在F上添加S得到的（F的）扩张，记为$F(S)$。也就是说，设

$$M=\{F_i \mid F_i\text{是}E\text{的子域且}F\subseteq F_i,\ S\subseteq F_i\}$$

则

$$F(S)=\bigcap_{F_i\in M}F_i$$

显然$F(S)$是E的子域，而且它是既包含F又包含S的最小的子域：$F(S)\in M$，并且$\forall F_i\in M$有$F(S)\subseteq F_i$。

下面我们来考虑，$F(S)$是E的哪些元素组成的，这些元素有什么特征。

命题1　设F是域E的子域，S是E的子集合，则

$$F(S)=\left\{\frac{f(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g(\alpha_1,\alpha_2,\cdots,\alpha_n)}\,\middle|\,\alpha_i\in S,\ f(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n),\right.$$

$\left.g(\alpha_1,\alpha_2,\cdots,\alpha_n)\neq 0,\ \text{是}\alpha_1,\alpha_2,\cdots,\alpha_n\text{在}F\text{上的多项式},\ n\text{是正整数}\right\}$

证明　设

$$K=\left\{\frac{f(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g(\alpha_1,\alpha_2,\cdots,\alpha_n)}\ \middle|\ \alpha_i\in S,\ f(\alpha_1,\alpha_2,\cdots,\alpha_n),g(\alpha_1,\alpha_2,\right.$$

$\left.\cdots,\alpha_n)\neq 0\text{是}\alpha_1,\alpha_2,\cdots,\alpha_n\text{在}F\text{上的多项式，}n\text{是正整数}\right\}$

显然K是E的一个含有非零元素的子集．对于K中任意二元素

$$k_1=\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g_1(\alpha_1,\alpha_2,\cdots,\alpha_n)},\quad k_2=\frac{f_2(\beta_1,\beta_2,\cdots\beta_m)}{g_2(\beta_1,\beta_2,\cdots,\beta_m)}$$

有

$$k_1-k_2=\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}-\frac{f_2(\beta_1,\beta_2,\cdots,\beta_m)}{g_2(\beta_1,\beta_2,\cdots,\beta_m)}$$

$$=\frac{f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)g_2(\beta_1,\beta_2,\cdots\beta_m)-f_2(\beta_1,\beta_2,\cdots,\beta_m)g_1(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g_1(\alpha_1,\alpha_2,\cdots,\alpha_n)g_2(\beta_1,\beta_2,\cdots,\beta_m)}$$

上面分式的分子和分母都是$\alpha_1,\alpha_2,,\cdots,\alpha_n,\beta_1,\beta_2,\cdots,\beta_m$在$F$上的多项式，而且分母不等于零，故

$$k_1-k_2\in K$$

同样可证，$\forall k_1,\ k_2\in K,\ k_2\neq 0$，有$k_1k_2^{-1}\in K$。于是$K$是$E$的子域。

其次证明：$F\subseteq K$，$S\subseteq K$。实事上，$\forall a\in F$，$\alpha\in S$均有

$$a=\frac{a}{1}\in K,\quad \alpha=\frac{\alpha}{1}\in K$$

因此推得$F(S)\subseteq K$。

反之，对K中任一元素

$$k=\frac{f(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g(\alpha_1,\alpha_2,\cdots,\alpha_n)}$$

因$f(\alpha_1,\alpha_2,,\cdots,\alpha_n),g(\alpha_1,\alpha_2,\cdots,\alpha_n)\in F(S)$，则有$k\in F(S)$，即$K\subseteq F(S)$。所以

$$F(S)=K$$

证完。

推论 设E是一个域，F是E的子域，$S=\{\alpha_1,\ \alpha_2,\cdots,\alpha_n\}$是$E$的有限子集，此时可记$F(S)=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，则

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=\left\{\frac{f(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g(\alpha_1,\alpha_2,\cdots,\alpha_n)}\ \middle|\ f(\alpha_1,\alpha_2,\cdots,\alpha_n),g(\alpha_1,\right.$$

$\alpha_2, \cdots, \alpha_n) \neq 0$是 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 在 F 上的多项式$\}$

特别地，当$S=\{\alpha\}$时，则有

$$F(\alpha)=\left\{\frac{f(\alpha)}{g(\alpha)}\ \middle|\ f(\alpha),\ g(\alpha)\neq 0 \text{是 } \alpha \text{ 在 } F \text{ 上的多项式}\right\}$$

定理1 设 F 是域 E 的子域，S，T都是 E 的子集，则

$$F(S\cup T)=F(S)(T)=F(T)(S)$$

证明 先证 $F(S\cup T)=F(S)(T)$。设 $F(S\cup T)=V$,则由定义1有$F,S\cup T\subseteq V$，从而$F,S,T\subseteq V$。由于V是E的子域并且包含F和S，所以$F(S)\subseteq V$。再因T是V的子集，在$F(S)$上添加T所得到的扩张 $F(S)(T)$ 被V包含，即 $F(S)(T)\subseteq V$，亦即 $F(S)(T)\subseteq F(S\cup T)$。

另一方面，设$F(S)(T)=W$，则由定义1有$F(S),T\subseteq W$，从而有 $F,S,T\subseteq W$，$F,S\cup T\subseteq W$。于是$F(S\cup T)\subseteq W$，即 $F(S\cup T)\subseteq F(S)(T)$。

因此

$$F(S\cup T)=F(S)(T)$$

同理可证

$$F(S\cup T)=F(T)(S)$$

证完。

定理1 可推广到n个子集的情形：设F是域E的子域，S_1，S_2，$\cdots$，S_n是E的n个子集，则

$$F(S_1\cup S_2\cup\cdots\cup S_n)=F(S_1)(S_2)\cdots(S_n)$$

特别地，当 $S_1=\{\alpha_1\}$，$S_2=\{\alpha_2\}$，$\cdots$，$S_n=\{\alpha_n\}$ 时，把$F(\{\alpha_1\})$记作$F_1(\alpha_1)$，则有

$$F(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$$

上述事实说明，在E的子域F上添加E的一个有限子集S，可以通过逐个添加S的元素而得到，并且与添加的顺序无关。

为了进一步讨论域的扩张，下面引进代数元和超越元概念。

定义2 设E/F(即F是域E的子域)，$\alpha\in E$，如果在$F[x]$中存在非零多项式$\varphi(x)$，使得

$$\varphi(\alpha)=0$$

则 α 叫做 F 上的代数元；如果对 $F[x]$ 中任一非零多项式 $\varphi(x)$ 均有

$$\varphi(\alpha)\neq 0$$

则 α 叫做 F 上的超越元。

例如，有理数域Q是复数域 C 的子域，$\sqrt{2}$，$i\in C$分别是Q上的多项式x^2-2，x^2+1的根，所以$\sqrt{2}$，i 都是Q上的代数元。$\pi\in C$是Q上的越超元。但 π 是R上的多项式$x-\pi$的根，所以 π 是实数域上的代数元。

再如，设E/F，$\forall \alpha\in F$，因 α 是 F 上的多项式$x-\alpha$的根，所以 F 的每个元素 α 都是 F 上的代数元。

定义 3　设 E/F，如果E 的每个元素都是 F 上的代数元，则 E 叫做 F 的代数扩张；如果 E 中存在 F 上的超越元，则 E 叫做 F 的超越扩张。

显然域F的任一扩张不是代数扩张就是超越扩张。这样一来，域的扩张可分成代数扩张和超越扩张两大类型。后几节，我们将侧重对代数扩张的讨论。为此在这里对代数元的有关性质做进一步介绍，以备后面使用。

定义 4　设 α 是域 F 上的代数元，则在 $F[x]$ 里以 α 为根的多项式中，首项系数为1，次数最小的多项式叫做 α 在 F 上的最小多项式。

例如，　x^2-2，x^2+1分别是$\sqrt{2}$，i 在Q上的最小多项式。

命题 2　域 F 上的代数元 α 在 F 上的最小多项式 $\varphi(x)$ 整除$F[x]$中任一以 α 为根的多项式$f(x)$。

证明　由带余除法可得

$$f(x)=q(x)\varphi(x)+r(x)$$

其中$r(x)=0$或者$\deg r(x)<\deg\varphi(x)$。

假设$\deg r(x)<\deg\varphi(x)$，则因为

$$f(\alpha)=q(\alpha)\varphi(\alpha)+r(\alpha)=0$$

从而有

$$r(\alpha)=0$$

这与 $\varphi(x)$ 是 α 的最小多项式相矛盾。所以只能 $r(x)=0$，即 $\varphi(x)\mid f(x)$。证完。

命题 3　域 F 上的代数元 α 在 F 上有唯一的最小多项式。

证明　α 在 F 上的最小多项式的存在性是明显的。现证明唯一性。设 $\varphi_1(x)$，$\varphi_2(x)\in F[x]$ 都是 α 的最小多项式，由命题 2 有

$$\varphi_2(x)=q_1(x)\varphi_1(x) \tag{1}$$

$$\varphi_1(x)=q_2(x)\varphi_2(x)$$

于是

$$\varphi_2(x)=q_1(x)q_2(x)\varphi_2(x)$$

$$q_1(x)q_2(x)=1$$

从而得知 $q_1(x)$ 是零次多项式。再因 $\varphi_1(x)$ 和 $\varphi_2(x)$ 的首项系数都是 1，所以比较（1）式等号两端的首项系数可知 $q_1(x)=1$，故

$$\varphi_2(x)=\varphi_1(x)$$ 证完。

命题 4　域 F 上的代数元 α 的最小多项式 $\varphi(x)$ 是 F 上不可约多项式。

证明　假设 $\varphi(x)$ 在 F 上可约，则必存在 $f_1(x)$，$f_2(x)\in F[x]$ $0<\deg f_1(x)$，$\deg f_2(x)<\deg\varphi(x)$，使得

$$\varphi(x)=f_1(x)f_2(x)$$

于是

$$\varphi(\alpha)=f_1(\alpha)f_2(\alpha)=0$$

这时必有 $f_1(\alpha)=0$ 或 $f_2(\alpha)=0$，这与 $\varphi(x)$ 是 α 的最小多项式相矛盾。故 $\varphi(x)$ 在 F 上不可约。证完。

命题 5　设 F，E，K 都是域，且 $F\subseteq E\subseteq K$，如果 $\alpha\in K$ 是 F 上的代数元，则 α 必是 E 上的代数元。

事实上，此时存在非零多项式 $\varphi(x)\in F[x]$，使

$$\varphi(\alpha)=0$$

因 $F[x]\subseteq E[x]$，故 $\varphi(x)\in E[x]$，即 α 是 E 上的代数元。证完。

值得注意的是，E 上的代数元不一定是 F 上的代数元；即使 $\alpha\in K$ 同时是 F 上、E 上的代数元，但 α 在 F 上的最小多项式和 α 在 E 上的最小多项式也可能不相同。

例如，$\boldsymbol{Q}\subset\boldsymbol{R}\subset\boldsymbol{C}$，$\pi$ 是 $\boldsymbol{R}$ 上的代数元，但 π 是 $\boldsymbol{Q}$ 上的超越元。又如，$\sqrt{2}$ 在 $\boldsymbol{Q}$ 上，$\boldsymbol{R}$ 上都是代数元．但 $\sqrt{2}$ 在 $\boldsymbol{Q}$ 上，$\boldsymbol{R}$ 上的最小多项式分别为 x^2-2，$x-\sqrt{2}$。

习　　题

1　已知 π 和 $e=2.71828\cdots$ 是有理数域 $\boldsymbol{Q}$ 上的超越元，试判断下列复数在 $\boldsymbol{Q}$ 上是代数的还是超越的，并给出其证明：$\sqrt{5}$，$\sqrt[3]{7}$，π^2，$e+3$，i，$i+3$。

2　证明：d 是 $\boldsymbol{Q}$ 上的代数元 $\Longleftrightarrow d^2$ 和 $d+3$ 是 $\boldsymbol{Q}$ 上的代数元。

3　设 F 和 S 分别是域 E 的子域和子集，则 S 的一切有限子集添加到 F 上所得子域的并是一个域。

4　若域 F 上的代数元 α 是 $F[x]$ 中首项系数为 1 的不可约多项式 $\varphi(x)$ 的根，则 $\varphi(x)$ 是 α 在 F 上的最小多项式。

5　求下列两个扩张添加元素的最小多项式：$\boldsymbol{C}/\boldsymbol{R}$，$\boldsymbol{Q}(\sqrt[5]{3})$。

§3　单纯扩张

在这节里，我们讨论域的一类最简单的扩张：在域 E 的子域 F 上添加 E 的一个元素得到的扩张。

定义 1　**设 F 是域 E 的子域，$\alpha\in E$．则 $F(\alpha)$ 叫做 F 的单纯扩张。当 α 是 F 上的代数元时，$F(\alpha)$ 叫做 F 的单纯代数扩张；当 α 是 F 上的超越元时，$F(\alpha)$ 叫做 F 的单纯超越扩张。**

显然单纯超越扩张是超越扩张。下节将证明单纯代数扩张是代数扩张。现在我们来研究单纯扩张的结构，给出关于单纯扩张的重要结果。

定理 1　**设 F 是域 E 的子域，$\alpha\in E$．如果 $F(\alpha)$ 是 F 的单**

纯超越扩张，则$F(\alpha)\cong F(x)$；如果$F(\alpha)$是F的单纯代数扩张，则$F(\alpha)\cong F[x]/(\varphi(x))$，其中$\varphi(x)$是$\alpha$在$F$上的最小多项式。

证明 由§2 命题1的推论知

$$F(\alpha)=\left\{\frac{f(\alpha)}{g(\alpha)}\;\middle|\; f(x),\ g(x)\in F[x],\ g(x)\neq 0\right\}$$

考虑$F(\alpha)$的子集

$$F[\alpha]=\{f(\alpha)\mid f(x)\in F[x]\}$$

显然$F[\alpha]$是$F(\alpha)$的子环，而且$F[\alpha]$是整环，$F[\alpha]$的商域恰好是$F(\alpha)$。我们来比较$F[x]$与$F[\alpha]$，令

$$\Psi: f(x)\longmapsto f(\alpha)$$

显然Ψ是$F[x]$到$F[\alpha]$的满射，而且$\forall f(x)$，$g(x)\in F[x]$，有

$$\Psi: f(x)+g(x)\longmapsto f(\alpha)+g(\alpha)$$

$$f(x)g(x)\longmapsto f(\alpha)g(\alpha)$$

故Ψ是$F[x]$到$F[\alpha]$的满同态。由第三章知，Ψ的核$N=\ker\Psi$是$F[x]$的理想，而多项式环$F[x]$是主理想环，所以$N=(\varphi(x))$。若$\varphi(x)\neq 0$，则令$\varphi(x)$的首项系数为1。下面分两种情况进行讨论。

（1）当α是F上的超越元，此时对任一非零多项式$f(x)\in F[x]$均有$f(\alpha)\neq 0$，于是$N=\{0\}$，故

$$\Psi: F[x]\cong F[\alpha]$$

进而由第三章§8定理3知，$F[x]$的商域$F(x)$与$F[\alpha]$的商域$F(\alpha)$同构：

$$F(x)\cong F(\alpha)$$

（2）当α是F上的代数元，此时$N=(\varphi(x))\neq\{0\}$，$\varphi(x)\neq 0$。由核的定义知，N恰是由$F[x]$中以α为根的所有多项式组成的集合。$\varphi(x)$是N中的多项式又能整除以α为根的所有多项式，可见，$\varphi(x)$是首项系数为1，次数最小的，以α为根的多项式。故$\varphi(x)$是α的最小多项式。由第三章环的同态基本定理知

$$F[x]/(\varphi(x))\overset{\sigma}{\cong}F[\alpha]$$

其中σ：$\overline{f(x)} = f(x) + (\varphi(x)) \longmapsto f(\alpha)$。

由于$\varphi(x)$是$F[x]$中不可约多项式，故$N = (\varphi(x))$是$F[x]$中的极大理想，再由第三章§7定理1知$F[x]/(\varphi(x))$是域。于是$F[\alpha]$必是域，此时$F[\alpha] = F(\alpha)$，因此

$$F[x]/(\varphi(x)) \cong F(\alpha)$$

证完。

推论 设F是域，如果α，β都是F上的超越元，则$F(\alpha) \cong F(\beta)$；如果α，β都是F上的代数元，而且它们在F上的最小多项式相同，则$F(\alpha) \cong F(\beta)$。

此推论中的α，β不必是同一个域中的元素。

定理1比较清楚地说明了单纯扩张的结构。对单纯超越扩张$F(\alpha)$来说，$F(\alpha)$中元素之间的运算与$F(x)$中元素之间的运算一致，可以把α看做是未定元做有理分式运算；对于单纯代数扩张$F(\alpha)$来说，我们看到，对$F(\alpha)$的结构起决定性作用的是α的最小多项式$\varphi(x)$。下面就后一情况做进一步的讨论。

定理2 设$F(\alpha)$是F的单纯代数扩张，$\varphi(x)$是α在F上的最小多项式，其次数为n。则$F(\alpha)$的每个元素$\dfrac{f(\alpha)}{g(\alpha)}$都可唯一地表为

$$\frac{f(\alpha)}{g(\alpha)} = \sum_{i=0}^{n-1} = a_i\alpha^i = h(\alpha),\quad a_i \in F \qquad (1)$$

而且对于 $h_1(\alpha) = \sum_{i=0}^{n-1} a_i\alpha^i$，　$h_2(\alpha) = \sum_{i=0}^{n-1} b_i\alpha^i$有

$$h_1(\alpha) + h_2(\alpha) = \sum_{i=0}^{n-1}(a_i + b_i)\alpha^i$$

$$h_1(\alpha)h_2(\alpha) = r(\alpha)$$

其中$r(x)$是以$\varphi(x)$除$h_1(x)h_2(x)$所得的余式。

证明 我们来证明定理的前一个结论。在定理1的证明中已经看到，此时$F(\alpha) = F[\alpha]$。于是，$\forall \dfrac{f(\alpha)}{g(\alpha)} \in F(\alpha)$：均有$k(\alpha) \in F[\alpha]$，使

$$\frac{f(\alpha)}{g(\alpha)}=k(\alpha)$$

由带余除法得

$$k(x)=q(x)\varphi(x)+h(x)$$

其中

$$h(x)=\sum_{i=0}^{n-1}a_i x^i,\quad a_i\in F$$

因 $\varphi(\alpha)=0$，故

$$\frac{f(\alpha)}{g(\alpha)}=k(\alpha)=h(\alpha)=\sum_{i=1}^{n-1}a_i\alpha^i$$

对于$\frac{f(\alpha)}{g(\alpha)}$来说，表法（1）是唯一的．事实上，如果还有

$$\frac{f(\alpha)}{g(\alpha)}=h'(\alpha)=\sum_{i=0}^{n-1}a'_i\alpha^i,\quad a'_i\in F$$

则

$$h(\alpha)-h'(\alpha)=0$$

此时必有 $h(x)=h'(x)$。否则假设 $h(x)\neq h'(x)$，则 $h(x)-h'(x)\neq 0$，但$h(x)-h'(x)$的次数小于 n，且 $h(\alpha)-h'(\alpha)=0$ 这与 α 的最小多项式$\varphi(x)$是 n 次多项式相矛盾．因此

$$h(x)=h'(x)$$

故

$$a_i=a'_i$$

定理的后一个结论的证明比较简单，请读者自行完成．证完．

定理 2 告诉我们，单纯代数扩张$F(\alpha)$中的元素存在简捷的表示形式，而且给出了在该形式之下元素间运算法则．

例 3 有理数域 Q 是实数域 R 的子域，$\sqrt{2}\in R$ 是 Q 上的代数元，$\sqrt{2}$ 在 Q 上的最小多项式为 $\varphi(x)=x^2-2$，其次数为 2，于是$Q(\sqrt{2})$中的每个元素 u 均可表成

$$u=a+b\sqrt{2},\quad a,\ b\in Q$$

而且，$\forall u,\ v\in Q(\sqrt{2})$，$u=a+b\sqrt{2}$，$v=c+d\sqrt{2}$，$a,b,$

c，$d\in Q$，有

$$u+v=(a+b\sqrt{2})+(c+d\sqrt{2})$$
$$=(a+c)+(b+d)\sqrt{2}$$
$$uv=(a+b\sqrt{2})(c+d\sqrt{2})$$
$$=(ac+2bd)+(ad+bc)\sqrt{2}$$

上面我们所讨论的单纯扩张都是在一个域 E 的子域 F 上添加 E 的一个元素得到的。如果先任意给定一个域 F，是否一定存在 F 的扩张 E，使得在 F 上添加 E 的一个元素而得到不同于 F 的 F 的单纯扩张呢？回答是肯定的。

首先，F 的单纯超越扩张的存在性比较容易说明。我们知道，对任意一个域 F，必然存在多项式环 $F[x]$ 以及 $F[x]$ 的商域，即 F 上的有理分式域。这个域是以 F 为子域的，而它的元素 x 是 F 上的超越元，所以 $F(x)$ 是 F 的单纯超越扩张。实际上 $F(x)$ 就是 F 上的有理分式域。

其次对于 F 的单纯代数扩张的存在性，我们有

定理 3 **设 F 是任一域，$\varphi(x)$ 是 F 上首项系数为 1 的不可约多项式，则存在 F 的单纯代数扩张 $F(\alpha)$，其中 α 在 F 上的最小多项式为 $\varphi(x)$。**

证明 设 $\varphi(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$。由于 $\varphi(x)$ 是 $F[x]$ 中不可约多项式，则 $\varphi(x)$ 生成的理想 $(\varphi(x))$ 是 $F[x]$ 的极大理想。于是由第三章 § 7 定理 1，商环 $F[x]/(\varphi(x))$ 是域，我们已经知道，存在自然同态

$$\Psi: F[x]\sim F[x]/(\varphi(x))$$

其中

$$\Psi: f(x)\longmapsto \overline{f(x)}=f(x)+(\varphi(x))$$

设 $\Psi(F)=\overline{F}$，显然 $\overline{F}$ 是域 $F[x]/(\varphi(x))$ 的子域。

这时 Ψ 可以看做是 F 到 $\overline{F}$ 的映射，而且是双射。事实上，$\forall a, b\in F$，$a\neq b$，则 $a-b\neq 0$，而 $\varphi(x)$ 是 $F[x]$ 中的不可约多项式，其次数 $n>0$，所以 $\varphi(x)\nmid a-b$。从而 $a-b\notin(\varphi(x))$。因为 $\ker\Psi=(\varphi(x))$，故 $\overline{a-b}\neq\overline{0}$，于是得到 $\overline{a}\neq\overline{b}$。因此

$$\Psi: F \cong \overline{F}$$

应用第三章§6定理3，把$F[x]/(\varphi(x))$中的$\overline{F}$用F替换得到E，

$$F \subseteq E \text{且} E \cong F[x]/(\varphi(x))$$

其中

$$\nu: \overline{f(x)} \longmapsto \overline{f(x)}, \text{当} \overline{f(x)} \in \overline{F}$$

$$a \longmapsto \overline{a}, \text{当} a \in F$$

我们来观察$F[x]/(\varphi(x))$中的元素$\overline{x}$在ν之下的原象$\alpha \in E$由于

$$\overline{\varphi(x)} = \overline{x^n + a_{n-1}x^{n-1} + \cdots + a_n} = 0$$

再因Ψ是同态映射，则有

$$\overline{x}^n + \overline{a}_{n-1}\overline{x}^{n-1} + \cdots + \overline{a}_n = 0$$

又因ν是同构映射，便有

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_n = 0$$

即

$$\varphi(\alpha) = 0$$

这说明E中的元素α是以$\varphi(x)$为最小多项式的F上的代数元，$F(\alpha)$就是所要求的F的单纯代数扩张，证完。

对于上述证明中所得到的添加元α，我们需要进一步明确：当给定的不可约多项式$\varphi(x)$是一次多项式时，则有$\alpha \in F$，此时$F(\alpha) = F$；当$\varphi(x)$的次数$\geqslant 2$时，必有$\alpha = \overline{x}$，此时$F(\alpha) = F(\overline{x})$。

习　　题

1　设F为任一域，x是F上的未定元，$\Sigma = F(x)$，$\Delta = F\left(\frac{x^3}{x+1}\right)$，证明：$\Sigma$是$\Delta$的是单纯代数扩张。

2　试将$\mathbf{Q}(\sqrt[3]{2})$中的元素$\alpha = \frac{1+\sqrt[3]{2}}{1+\sqrt[3]{2}+\sqrt[3]{4}}$化成$\sqrt{2}$在$\mathbf{Q}$上的次数小于3的多项式。

3　设α是$\mathbf{R}$上多项式$g(x)=x^2+x+1$的根，求出单纯扩张 $\mathbf{R}(\alpha)$，并在$\mathbf{R}(\alpha)$上分解$g(x)$为不可约因子之积。

4　设F是特征数为p的素域，$K=F(x)$。

（1）证明：y^p-x在K上不可约。

（2）做出$K(\theta)$，θ的最小多项式为y^p-x。

（3）在$K(\theta)$上分解y^p-x为不可约因式之积。

§4　有限扩张

上节讨论了在域F上添加一个元素α所得到的单纯扩张$F(\alpha)$的结构，现在来研究在F上添加F上的有限个代数元α_1，α_2，…，α_n所得到的扩张$F(\alpha_1, \alpha_2, \cdots, \alpha_n)$的一些性质。对于添加有限个超越元的情形，超出本书范围，这里不予涉及。

对于添加有限个代数元的扩张的讨论，我们从另一个角度开始。读者已经熟习域上向量空间的理论。设E/F（即E是F的扩域），则E是F上的一个向量空间，这个空间的向量加法和F乘E的作用乘法分别是域E的加法和乘法。

定义1　**设F是域E的子域，如果E做为F上的向量空间是有限维的，则E叫做F的有限扩张，其维数记为(E/F)，叫做扩张次数。当$(E/F)=n$时，则说E是F的n次扩张。如果E做为F上的向量空间是无限维的，则E叫做F的无限扩张。**

例1　复数域C是实数域R的二次扩张。这是因为C做为R上的向量空间，1和i组成C的一组基底，维数为2，即$(C/R)=2$。

实数域R是有理数域Q的无限扩张。事实上，R做为Q上的线性空间是无限维的，这是因为，对于$\pi\in R$和任一正整数n，R中的n个向量

$$\pi^n, \ \pi^{n-1}, \ \cdots, \ \pi$$

在Q上是线性无关的。否则有Q中不全为零的数a_n，a_{n-1}，…，a_1使

$$a_n\pi^n + a_{n-1}\pi^{n-1} + \cdots + a_1\pi = 0$$

这说明π是Q上的多项式

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x$$

的根，与π是Q上的超越元相矛盾。由此可知，R中不存在有限个向量所构成的基底。因此R是Q的无限扩张。

命题 设$F(\alpha)$是域F的单纯代数扩张，α在F上最小多项式$\varphi(x)$的次数为n，则$F(\alpha)$是F的n次扩张。

证明 由§3定理2知，$F(\alpha)$的每个元素u都可唯一地表为

$$u = \sum_{i=0}^{n-1} a_i\alpha^i, \quad a_i \in F$$

所以$F(\alpha)$做为F上的向量空间来说，n个向量$1,\alpha,\cdots,\alpha^{n-1}$构成此空间的一个生成集。而且当

$$b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \cdots + b_0 = 0$$

时，必有$b_i = 0$，$i = 0,1,\cdots,n-1$。因此1，$\alpha,\cdots,\alpha^{n-1}$是线性无关向量组，从而是$F(\alpha)$的基底。于是$(F(\alpha)/F) = n$。证完。

定理1 设F，Δ，E是三个域，E是Δ的有限扩张，Δ是F的有限扩张，则E是F的有限扩张，而且

$$(E/F) = (E/\Delta)(\Delta/F)$$

证明 设$(\Delta/F) = m$，$(E/\Delta) = n$，$u_1,u_2,\cdots,u_m$是Δ在F上的基底，$v_1,v_2,\cdots,v_n$是E在Δ上的基底。我们来证明$\{u_iv_j\}$($i = 1,2,\cdots,m$；$j = 1,2,\cdots,n$)是E在F上的基底。$\forall u \in E$有

$$u = a_1v_1 + a_2v_2 + \cdots + a_nv_n, \quad a_i \in \Delta$$

因为

$$a_j = b_{1j}u_1 + b_{2j}u_2 + \cdots + b_{mj}u_m, b_{ij} \in F, \quad j = 1,2,\cdots,n,$$

所以

$$u = (b_{11}u_1 + b_{21}u_2 + \cdots + b_{m1}u_m)v_1 +$$
$$(b_{12}u_1 + b_{22}u_2 + \cdots + b_{m2}u_m)v_2 +$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(b_{1n}u_1 + b_{2n}u_2 + \cdots + b_{mn}u_m)v_n$$

$$= b_{11}u_1v_1 + b_{21}u_2v_1 + \cdots + b_{m1}u_mv_1 + \cdots +$$

$$+ b_{ij}u_iv_j + \cdots + b_{mn}u_mv_n.$$

上式说明$\{u_iv_j\}$是线性空间E（在F上）的生成集。其次证明$\{u_iv_j\}$在F上是线性无关的。设

$$\sum_{\substack{i=1,\cdots,m\\ j=1,\cdots,n}} b_{ij}u_iv_j = 0,\quad b_{ij}\in F$$

则

$$\sum_{j=1,\cdots,n}\left(\sum_{i=1,\cdots,m} b_{ij}u_i\right)v_j = 0$$

由于

$$\sum_{i=1,\cdots,m} b_{ij}u_i \in \Delta$$

且$\{v_j\}$在Δ上线性无关，故

$$\sum_{i=1,\cdots,m} b_{ij}u_i = 0,\quad j=1,\cdots,n$$

再因$\{u_i\}$在F上线性无关，得

$$b_{ij}=0,\quad i=1,\cdots,m;\ j=1,\cdots,n$$

综上所述，$\{u_iv_j\}$是E在F上的基底，而$\{u_iv_j\}$由mn个元素组成，所以E是F上的mn维向量空间，即E是F的有限扩张，$(E/F)=mn$。证完。

定理1可以推广到F和E之间存在有限个中间域的情形，利用数学归纳法可证

推论1 设$F,\Delta_1,\Delta_2,\cdots,\Delta_k,E$都是域，且$\Delta_1,\Delta_2,\cdots,\Delta_k$，$E$分别是$F,\Delta_1,\cdots,\Delta_k$的有限扩张，则$E$是$F$的有限扩张，而且

$$(E/F)=(\Delta_1/F)(\Delta_2/\Delta_1))\cdots E/\Delta_k)$$

关于有限扩张，还有以下几个重要性质。

定理2 有限扩张必是代数扩张。

证明 设E是F的有限扩张，$(E/F)=n$。要证E是F的代数扩张，只须证每个$u\in E$都是F上的代数元即可。因为F

上的向量空间E的维数是n，则$n+1$个向量

$$u^n,\ u^{n-1},\ \cdots,u,\ 1$$

必线性相关，于是在F中存在$n+1$个不全为0的元素$a_n,a_{n-1},\cdots,a_0$，使得

$$a_nu^n+a_{n-1}u^{n-1}+\cdots+a_0=0$$

这说明u是F上非零多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$

的根，即u是F上的代数元，从而E是F的代数扩张。证完。

由前面的命题知，单纯代数扩张是有限扩张，所以有

推论 2　单纯代数扩张必是代数扩张。

定理 3　设E/F是有限扩张，则$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，其中每个$\alpha_i$都是$F$上的代数元；反之，如果$\alpha_1,\alpha_2,\cdots,\alpha_n$都是域$F$上的代数元，则$F(\alpha_1,\alpha_2,\cdots,\alpha_n)$是$F$的有限扩张。

证明　设E是F的有限扩张．$\alpha_1,\alpha_2,\cdots,\alpha_n$是$E$在$F$上的基底．显然

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)\subseteq E$$

另一方面，$\forall\alpha\in E$，存在$a_1,a_2,\cdots,a_n\in F$，使得

$$\alpha=a_1\alpha_2+a_2\alpha_2+\cdots+a_n\alpha_n\in F(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

故

$$E\subseteq F(\alpha_1,\alpha_2,\cdots,\cdots,\alpha_n)$$

因此

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

由定理2知，每个α_i都是F上的代数元，从而定理的第一个结论得证。

其次证明第二个结论。设$\alpha_1,\alpha_2,\cdots,\alpha_n$都是$F$上的代数元，则

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$$

观察以下域的序列

$$F\subseteq F(\alpha_1)\subseteq F(\alpha_1)(\alpha_2)\subseteq\cdots\subseteq F(\alpha_1)(\alpha_2)\cdots(\alpha_{n-1})\subseteq(\alpha_1)(\alpha_2)\cdots(\alpha_n)$$

序列中每个域都是其前一个相邻域的单纯代数扩张，从而都是有限扩张。由定理1知，$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$是$F$的有限扩张。证完。

推论3 设$\alpha_1,\alpha_2,\cdots,\alpha_n$是域$F$上的代数元，则$F(\alpha_1,\alpha_2,\cdots\alpha_n)$是$F$的代数扩张。

推论4 设α_1,α_2是域F上的代数元，则$\alpha_1+\alpha_2,\alpha_1-\alpha_2,\alpha_1\alpha_2$ $\frac{\alpha_1}{\alpha_2}$ $(\alpha_2\neq0)$都是F上的代数元。

定理3表明，在域F上添加有限个代数元所得到的扩张和F的有限扩张这两个概念是一致的。但须注意，一般情况下，在 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 中，添加的代数元个数n与扩张次数(E/F)不一定相等。例如，$C=R(i)$，$(C/R)=2$

还应注意，定理2的逆命题不真，即存在代数扩张不是有限扩张。例如，$Q\subset C$，设S是C中所有Q上的代数元的集合。由定理3的推论2知，S是域。显然$Q\subset S$，所以S是Q的代数扩张。但S不是Q的有限扩张。这是因为，对于任意正整数n，在S中都能找到n个在Q上线性无关的向量。事实上，对任意正整数n，存在n次有理系数不可约多项式$\varphi(x)$（例如，x^n+2 就是Q上n次不可约多项式）。设α是$\varphi(x)$的根，则$\alpha\in S$。因$\varphi(x)$是α在Q上的最小多项式，故S中的n个元素

$$1,\alpha,\cdots,\alpha^{n-1}$$

在Q上线性无关。所以S不是Q的有限扩张。

习　题

1　设$(K/F)=n$，$\alpha\in K$在F上的最小多项式的次数为m，则$m\mid n$。

2　设E是域F的有限扩张，$(E/F)=n$。则，$\forall\alpha\in E$，$F(\alpha)$是F的单纯代数扩张，而且$(F(\alpha)/F)=m$是n的约数。

3　$(\mathbf{Q}(i,\sqrt{2})/\mathbf{Q})=?$

4　若$(K/\mathbf{Z}_p)=n$，则K是有限域，试确定K的元素个数。

5　设K是F的有限扩张，α是K上的代数元，则α是F上的代数

元。

§5 分裂域

在本章最后两节，我们利用有限扩张的理论来研究两类特殊的域：多项式的分裂域和有限域。这两类域在域论中，特别是在伽罗瓦理论中占有重要地位。

定义1 设$f(x)$是域F上的n（$\geqslant 1$）次多项式，F的扩张E如果满足

（1）$f(x)$如E上可分解为一次因子之积

$$f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

（2）E是在F上添加$f(x)$在E中的全部根得到的扩张

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

则E叫做$f(x)$的一个分裂域。

由定义可以看出，域F上的多项式$f(x)$的分裂域是包含$f(x)$的所有n个根的最小扩张。

例如，$f(x)=x^2+1$是有理数域Q上的多项式，$Q(i)$是F的扩张。$f(x)$在$Q(i)$上可分解为

$$f(x)=(x-i)(x+i)$$

$$Q(i)=Q(i,-i)$$

所以$Q(i)$是x^2+1的分裂域。

现在来讨论这样问题：对于域F上的任一n($\geqslant 1$)次多项式$f(x)$是否存在分裂域？如果存在，是否唯一。

首先证明分裂域的存在性。

定理1 域F上的任一n($\geqslant 1$)次多项式$f(x)$都有分裂域。

证明 对$f(x)$的次数n用数学归纳法。

当$n=1$时，$f(x)$是F上的一次多项式，它的根$\alpha\in F$，此时F便是$f(x)$的分裂域。

当$n>1$，假设$n-1$次多项式有分裂域。在F上把$f(x)$分解为

$$f(x)=\varphi(x)g(x)$$

其中 $\varphi(x)$ 是 F 上首项系数为 1 的不可约多项式。由 § 3 定理 3，存在 F 的单纯代数扩张 $F(\alpha_1)$，其中 α_1 在 F 上的最小多项式为 $\varphi(x)$。于是在 $F(\alpha_1)$ 上，$x-\alpha_1|\varphi(x)$ 从而 $x-\alpha_1|f(x)$。所以，在 $F(\alpha_1)$ 上，$f(x)$ 可分解为

$$f(x)=(x-\alpha_1)q(x)$$

其中，$q(x)$ 是 $F(\alpha_1)$ 上的 $n-1$ 次多项式。由归纳假设，存在 $q(x)$ 的分裂域 E，在 E 上 $q(x)$ 可分解为

$$q(x)=c(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_n)$$

而且

$$E=F(\alpha_1)(\alpha_2,\alpha_3,\cdots,\alpha_n)$$

E 就是 $f(x)$ 的分裂域，事实上，在 E 上 $f(x)$ 可分解为

$$f(x)=(x-\alpha_1)q(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

而且

$$E=F(\alpha_1)(\alpha_2,\cdots,\alpha_n)=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

证完。

现在来讨论分裂域的唯一性问题。其实对于域 F 上的一个多项式 $f(x)$ 来说，满足定义 1 的 F 的扩张即 $f(x)$ 的分裂域可以有许多，但是我们将证明，这些不同的分裂域相互同构。所以在同构的意义下，$f(x)$ 的分裂域是唯一的。为了讨论分裂域的唯一性，先引进同构开拓概念。

定义 2 设 F，$\widetilde{F}$，是两个域，$\sigma: F\cong\widetilde{F}$，$R$ 和 $\widetilde{R}$ 分别是 F 和 $\widetilde{F}$ 的扩环。如果存在 $\sigma': R\cong\widetilde{R}$，使得 $\forall a\in F$ 有 $\sigma'(a)=\sigma(a)$，那么，σ' 叫做 σ 在 R 到 $\widetilde{R}$ 上的同构开拓，简称 σ' 是 σ 的开拓。

引理 1 设 F，$\widetilde{F}$ 是两个域，$\sigma: F\cong\widetilde{F}$，则存在 σ 在 $F[x]$ 到 $\widetilde{F}[x]$ 上的同构开拓 σ'。

证明 $\forall a\in F$，设 $\sigma(a)=\widetilde{a}$。令

$\sigma': f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\longmapsto\widetilde{f}(x)=\widetilde{a}_nx^n+\widetilde{a}_{n-1}x^{n-1}+\cdots+\widetilde{a}_0$，$\forall f(x)\in F[x]$

显然σ'是$F[x]$到$\widetilde{F}[x]$的双射，并易证

$$\widetilde{f}(x)+\widetilde{g}(x)=\widetilde{f(x)+g(x)},\quad \widetilde{f}(x)\widetilde{g}(x)=\widetilde{f(x)g(x)}$$

故

$$\sigma':F[x]\cong\widetilde{F}[x]$$

并且，$\forall a\in F$，有

$$\sigma'(a)=\widetilde{a}=\sigma(a)$$

所以σ'是σ的开拓。证完。

为了说话方便起见，有时把$\sigma' f(x)=\widetilde{f}(x)$叫做$f(x)$在$\sigma$之下所对应的多项式。由于$\sigma$的开拓$\sigma'$是同构映射，所以当$f(x)$是$F[x]$中不可约多项式时，则在$\sigma$之下$f(x)$所对应的多项式$\widetilde{f}(x)$也是$\widetilde{F}[x]$中的不可约多项式。

引理 2 设F，$\widetilde{F}$是两个域，$\sigma:F\cong\widetilde{F}$，$\varphi(x)$是$F$上的首项系数为1的不可约多项式，$\widetilde{\varphi}(x)$是$\varphi(x)$在$\sigma$之下所对应的$\widetilde{F}$上的不可约多项式，$F(\alpha)$和$\widetilde{F}(\alpha)$分别是$F$和$\widetilde{F}$的单纯代数扩张，$\alpha$和$\widetilde{\alpha}$各在$F$和$\widetilde{F}$上的最小多项式是$\varphi(x)$和$\widetilde{\varphi}(x)$，则存在$\sigma$的同构开拓$\sigma':F(\alpha)\cong\widetilde{F}(\widetilde{\alpha})$，使得$\sigma'(\alpha)=\widetilde{\alpha}$。

证明 设$f(x)\in F[x]$在σ之下对应$\widetilde{f}(x)\in\widetilde{F}[x]$。根据§3定理1，存在

$$\sigma_1:F(\alpha)\cong F[x]/(\varphi(x))$$

其中

$$\sigma_1:h(\alpha)\longmapsto\overline{h(x)}=h(x)+(\varphi(x)),\quad\forall h(\alpha)\in F(\alpha)$$

同样存在

$$\sigma_2:\widetilde{F}[x]/(\widetilde{\varphi}(x))\cong\widetilde{F}(\widetilde{\alpha})$$

其中

$$\sigma_2:\overline{\widetilde{h}(x)}=\widetilde{h}(x)+(\widetilde{\varphi}(x))\longmapsto\widetilde{h}(\widetilde{\alpha}),$$

$$\forall\overline{\widetilde{h}(x)}\in\widetilde{F}[x]/(\widetilde{\varphi}(x))$$

令

$$\sigma_{12}:\overline{h(x)}\longmapsto\overline{\widetilde{h}(x)}$$

显然σ_{12}是$F[x]/(\varphi(x))$到$\widetilde{F}[x]/(\widetilde{\varphi}(x))$的双射，而且

$$\sigma_{12}(\overline{h(x)}+\overline{k(x)})=\sigma_{12}(\overline{h(x)+k(x)})=\overline{\widetilde{h}(x)+\widetilde{k}(x)}$$

$$=\overline{\widetilde{h}(x)}+\overline{\widetilde{k}(x)}=\overline{\widetilde{h}(x)}+\overline{\widetilde{k}(x)}\quad \sigma_{12}(\overline{h(x)})+\sigma_{12}(\overline{k(x)})$$

$$\sigma_{12}(\overline{h(x)}\,\overline{k(x)})=\sigma_{12}(\overline{h(x)k(x)})=\overline{\widetilde{h}(x)\widetilde{k}(x)}$$

$$=\overline{\widetilde{h}(x)}\,\overline{\widetilde{k}(x)}=\overline{\widetilde{h}(x)}\,\overline{\widetilde{k}(x)}=\sigma_{12}(\overline{h(x)})\sigma_{12}(\overline{k(x)})$$

故

$$\sigma_{12}:F[x]/(\varphi(x))\cong\widetilde{F}[x]/(\widetilde{\varphi}(x))$$

令$\sigma'=\sigma_2\sigma_{12}\sigma_1$，则因$\sigma_1,\sigma_{12},\sigma_2$都是同构映射故有

$$\sigma':F(\alpha)\cong\widetilde{F}(\widetilde{\alpha})$$

并且$\forall a\in F$，有

$$\sigma'(a)=\sigma_2(\sigma_{12}(\sigma_1(a)))=\sigma_2(\sigma_{12}(\overline{a}))=\sigma_2(\overline{\widetilde{a}})=\widetilde{a}=\sigma(a)$$

故σ'是σ的开拓。同时

$$\sigma'(\alpha)=\sigma_2(\sigma_{12}(\sigma_1(\alpha)))=\sigma_2(\sigma_{12}(\overline{x}))=\sigma_2(\overline{\widetilde{x}})=\widetilde{\alpha}$$

证完。

现在证明比描述分裂域唯一性更一般的

定理 2 设F，$\widetilde{F}$是两个域，$\sigma:F\cong\widetilde{F}$，$f(x)$是$F$上的$n(\geqslant 1)$次多项式，$\widetilde{f}(x)$是$f(x)$在$\sigma$之下对应的多项式，$F(\alpha_1,\alpha_2,\cdots,\alpha_n)$和$\widetilde{F}(\widetilde{\alpha}_1,\widetilde{\alpha}_2,\cdots,\widetilde{\alpha}_n)$分别是$f(x)$和$\widetilde{f}(x)$各在$F$和$\widetilde{F}$上的分裂域，则存在$\sigma$的同构开拓，$\sigma':F(\alpha_1,\alpha_2,\cdots,\alpha_n)\cong\widetilde{F}(\widetilde{\alpha}_1,\widetilde{\alpha}_2,\cdots,\widetilde{\alpha}_n)$，而且经适当调整顺序有$\sigma'(\alpha_i)=\widetilde{\alpha}_i$，$i=1,2,\cdots,n$。

证明 对$f(x)$的次数n用数学归纳法。

当$n=1$时，$f(x)$和$\widetilde{f}(x)$分别是F和$\widetilde{F}$上的一次多项式，它们的根$\alpha_1\in F$，$\widetilde{\alpha}_1\in\widetilde{F}$，于是它们的分裂域$F(\alpha_1)=F$，$\widetilde{F}(\widetilde{\alpha}_1)=\widetilde{F}$，并且容易证明$\sigma(\alpha_1)=\widetilde{\alpha}_1$，所以这时$\sigma$自身就是满足定理条件的同构开拓。

当$n>1$，假设定理对于$n-1$成立。由于α_1是$f(x)$的根，则α_1在F上的最小多项式$\varphi(x)$整除$f(x)$

$$f(x)=\varphi(x)g(x)$$

$\varphi(x)$，$g(x)$在σ之下所对应的多项式$\widetilde{\varphi}(x)$，$\widetilde{g}(x)$使

$$\widetilde{f}(x)=\widetilde{\varphi}(x)\widetilde{g}(x)$$

其中$\widetilde{\varphi}(x)$是$\widetilde{F}$上的首项系数为1的不可约多项式．在$\widetilde{f}(x)$的n个根$\widetilde{\alpha}_1,\widetilde{\alpha}_2,\cdots,\widetilde{\alpha}_n$中必有$\widetilde{\varphi}(x)$的根，不妨设$\widetilde{\alpha}_1$是$\widetilde{\varphi}(x)$的根．于是$\widetilde{\varphi}(x)$是$\widetilde{\alpha}_1$在$\widetilde{F}$上的最小多项式．

由引理2，存在σ的开拓

$$\sigma_1: F(\alpha_1)\cong\widetilde{F}(\widetilde{\alpha}_1)$$

使得$\sigma_1(\alpha_1)=\widetilde{\alpha}_1$．

在$F(\alpha_1)$和$\widetilde{F}(\widetilde{\alpha}_1)$上，$f(x)$和$\widetilde{f}(x)$可分别分解为

$$f(x)=(x-\alpha_1)q(x),\quad \widetilde{f}(x)=(x-\widetilde{\alpha}_1)\widetilde{q}(x)$$

其中$\widetilde{q}(x)$是$q(x)$在σ_1之下所对应的多项式，$q(x)$和$\widetilde{q}(x)$分别是$F(\alpha_1)$和$\widetilde{F}(\widetilde{\alpha}_1)$上的$n-1$次多项式，而且$\alpha_2,\cdots,\alpha_n$和$\widetilde{\alpha}_2,\cdots,\widetilde{\alpha}_n$分别是它们的$n-1$个根，所以

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2,\cdots,\alpha_n)$$

和

$$\widetilde{F}(\widetilde{\alpha}_1,\widetilde{\alpha}_2,\cdots,\widetilde{\alpha}_n)=\widetilde{F}(\widetilde{\alpha}_1)(\widetilde{\alpha}_2,\cdots,\widetilde{\alpha}_n)$$

分别是$q(x)$和$\widetilde{q}(x)$各在$F(\alpha_1)$和$\widetilde{F}(\widetilde{\alpha}_1)$上的分裂域．

由归纳假设，存在σ_1的同构开拓

$$\sigma': F(\alpha_1)(\alpha_2,\cdots,\alpha_n)\cong\widetilde{F}(\widetilde{\alpha}_1)(\widetilde{\alpha}_2,\cdots,\widetilde{\alpha}_n)$$

$$(\text{即}F(\alpha_1,\alpha_2,\cdots,\alpha_n)\cong\widetilde{F}(\widetilde{\alpha}_1,\widetilde{\alpha}_2,\cdots,\widetilde{\alpha}_n))$$

使得经适当调整顺序后有$\sigma'(\alpha_i)=\widetilde{\alpha}_i$，$i=1,2,\cdots,n$．同时有$\sigma'(\alpha_1)=\sigma_1(\alpha_1)=\widetilde{\alpha}_1$，显然$\sigma'$是满足定理条件的$\sigma$的同构开拓．证完．

推论　域F上的$n(\geqslant1)$次多项式$f(x)$的任意两个分裂域E和E'同构：$\sigma' E\cong E'$．其中σ'使F的元素不变，使$f(x)$在E中的根分别与在E'中的根相对应．

在定理2中取$\widetilde{F}=F$，取σ为F的恒等变换即得此推论．

分裂域的唯一性表明，域F上的多项式$f(x)$尽管在两个不

同的分裂域中各有一组根，但是这两组根没有本质差别。比如重根的个数，重根的重数，根与根之间由运算表示的关系等都是一致的。

例 1 试求$f(x)=x^4+1$在Q上的分裂域。

解 $f(x)$的根为 $\alpha_1=\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$, $\alpha_2=\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i$, $\alpha_3=-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$, $\alpha_4=-\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i$。

因为$\alpha_2=\alpha_1^{-1}, \alpha_3=-\alpha_1^{-1}, \alpha_4=-\alpha_1$，所以$f(x)$的分裂域为

$$Q(\alpha_1,\alpha_2,\alpha_3,\alpha_4)=Q(\alpha_1)$$

例 2 设F是特征数为p的域．$K=F(\alpha)$ 是单纯代数扩张，α是F上的多项式$f(x)=x^p-a$的根。证明K是$f(x)$在F上的分裂域。

证明 由于$f(\alpha)=\alpha^p-a=0$，所以$a=\alpha^p$，于是在K上有

$$f(x)=x^p-\alpha^p=(x-\alpha)^p$$

即α是$f(x)$的p重根，故$f(x)$在F上的分裂域

$$F(\alpha,\alpha,\cdots,\alpha)=F(\alpha)$$

习　　题

1 求$f(x)=x^3-5x^2+9x-9$在$\mathbf{Q}$上的分裂域。

2 设α是$\mathbf{Q}$上不可约多项式$\varphi(x)=x^3-a$的根，证明$\mathbf{Q}(\alpha)$不是$\varphi(x)$的分裂域。

3 设$\varphi_1(x)$，$\varphi_2(x)$，$\cdots$，$\varphi_m(x)$是域F上m个首项系数为1的不可约多项式。证明：存在F的有限扩张$F(\alpha_1,\alpha_2,\cdots,\alpha_m)$，其中$\alpha_i$在$F$上的最小多项式为$\varphi_i(x)$，$i=1,2,\cdots,m$。

4 设F是域。证明：F上的n次多项式$f(x)$在F上的分裂域E关于F的次数$\leqslant n!$。

§6　有　限　域

最后讨论有限域的结构．所谓有限域，就是元素个数有限

的域。首先我们注意，由§1定理1的推论3知，有限域的特征数为p，而§1的讨论告诉我们，有限域可以看做是$\mathbf{Z}_p$的扩张，进而由§4知，有限域是$\mathbf{Z}_p$的有限扩张，为了进一步研究有限域的结构，先来讨论素域Z_p上h次单位根的性质。

定义1 设h是与素数p互素的正整数，则$f(x)=x^h-1$叫做Z_p上的h次单位多项式，$f(x)$（在Z_p的任一扩张E中）的根叫做Z_p上的h次单位根。

命题1 Z_p上的h次单位多项式$f(x)=x^h-1$无重根。

证明 因为

$$f'(x)=hx^{h-1}\neq 0$$

则$f(x)$和$f'(x)$无公根，所以$f(x)$无重根。证完。

命题2 设E是Z_p的任一扩张，则E中所有Z_p上的h次单位根关于E的乘法构成交换群。

证明 只须证明$H=\{a\in E\,|\,a^h=1\}$是乘法群$\dot{E}$（E中非零元集合）的子群即可。

因为E中的1有性质：$1^h=1$，则$1\in H$，所以H非空。

进而，$\forall\,\alpha,\beta\in H$，因为$\alpha^h=\beta^h=1$，则有

$$(\alpha\beta^{-1})^h=\alpha^h(\beta^{-1})^h=\alpha^h(\beta^h)^{-1}=1$$

所以$\alpha\beta^{-1}\in H$。于是H是E的子群，由于域的乘法满足交换律，故H是交换群。证完。

做为命题2的直接结果，在x^h-1的分裂域E中，全体h个h次单位根构成E的子群。进一步还有

命题3 设E是Z_p的扩张，如果E含有Z_p上的全部h个h次单位根，则这些单位根的集合H关于E的乘法构成循环群。

证明 由命题1和命题2，已知H是h阶交换群。所以要证H是循环群，只须在H中找到阶为h的元素即可。

当$h=1$，此时$H=\{1\}=(1)$。

当$h>1$时，将h做标准分解

$$h=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$$

考虑下列一组多项式

$$f_i(x) = x^{\frac{h}{p_i}} - 1, \quad i = 1, 2, \cdots, s.$$

令 α 是 $f_i(x)$ 的根。则由 $\alpha^{\frac{h}{p_i}} = 1$ 得 $\alpha^h = \alpha^{\left(\frac{h}{p_i}\right)p_i} = 1$，即 $\alpha \in H$。所以每个 $f_i(x)$ 的根都是 h 次单位根。

但是，$\dfrac{h}{p_i} < h$，故在 H 中必存在 α_i，使得

$$\alpha_i^{\frac{h}{p_i}} \neq 1$$

令 $\beta_i = \alpha_i^{\frac{h}{p_i^{r_i}}}$，显然 $\beta_i \in H$，现在去求 β_i 在 H 中的阶。首先因为

$$\beta_i^{p_i^{r_i}} = \alpha_i^h = 1$$

其次由于

$$\beta_i^{p_i^{r_i-1}} = \alpha_i^{\frac{h}{p_i}} \neq 1$$

所以对于 $p_i^{r_i}$ 的每个小于其自身的正因数 q 来说，

$$\beta_i^q \neq 1$$

因此 β_i 在 H 中的阶为 $p_i^{r_i}$。

最后指出，如此求得的 s 个 β_i 之积

$$\gamma = \beta_1\beta_2\cdots\beta_s \in H$$

在 H 中的阶是 h。

事实上，因为 $p_1^{r_1}$，$p_2^{r_2}, \cdots, p_s^{r_s}$ 两两互素，所以

$$\gamma \text{ 的阶} = p_1^{r_1}, p_2^{r_2} \cdots p_s^{r_s} = h$$

于是 $H = (\gamma)$。证完。

现在讨论有限域的性质。首先考虑，有限域做为它所含素域的有限扩张的扩张次数、该有限域的元素个数以及其特征数之间的关系。对此有

定理 1 设 E 是 q 个元素的有限域，其特征数为 p，$(E/Z_p) = n$，则

$$q = p^n$$

证明 设 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 E 在 Z_p 上的基底，$\forall \beta \in E$ 有

$$\beta = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n, \quad a_i \in Z_p$$

而且表法唯一。而每个分量 a_i 各有种 p 取法，所以这种组合共

有p^n种取法，所以E所含元素的个数$q=p^n$。证完。

定理 2 设E是q元有限域，其特征数为p，则E是多项式$f(x)=x^q-x$在Z_p上的分裂域。

证明 设$E=\{\alpha_1,\alpha_2,\cdots,\alpha_q\}$，由于$E$的元素个数为$q$，则$\{\dot{E};\cdot\}$是$q-1$阶群，于是$\forall\alpha_i\in\dot{E}$都有

$$\alpha_i^{q-1}=1$$

从而

$$\alpha_i^q-\alpha_i=0$$

即α_i是$f(x)$的根。所以E中所有$q-1$个非零元素都是$f(x)$的根。此外，E中的元素0显然是$f(x)$的根。因此，E中的全部q个元素都是$f(x)$的根。于是在E上，$f(x)$可分解为

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_q)$$

另外，由于E的特征数为p，Z_p是E的子域，故有

$$E=Z_p(\alpha_1,\alpha_2,\cdots,\alpha_q)$$

综上所述可知E是$f(x)=x^q-x$在Z_p上的分裂域。证完。

做为此定理的直接结果，可得到

推论 1 元素个数相等的任二有限域必同构。

证明 设E_1,E_2都是q元有限域，由定理1有$q=p^n$，这说明E_1和E_2具有相同的特征数p，于是它们含有相同的素域Z_p。由定理2知，E_1和E_2都是$f(x)=x^q-x$在Z_p上的分裂域。再由§5定理2的推论即得$E_1\cong E_2$。证完。

定理1是说，任一有限域的元素个数必是一个素数的正整数次幂。反之，对于任一素数的任一正整数次幂来说，是否存在以此数为元素个数的有限域呢？对此有

定理 3 对于任一素数p和任一正整数n，必存在一个恰含$q=p^n$个元素的有限域E。

证明 由§5定理1知，Z_p上的多项式$f(x)=x^q-x$存在分裂域E。这时$f(x)$，在E上可分解为

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_q)$$

而且

$$E = Z_p(\alpha_1, \alpha_2, \cdots, \alpha_q)$$

下面证明E的元素个数为q．设

$$E' = \{\alpha_1, \alpha_2, \cdots, \alpha_q\} \subseteq E$$

因为，$\forall \alpha_i, \alpha_j \in E'$有

$$(\alpha_i - \alpha_j)^{p^n} = \alpha_i^{p^n} - \alpha_j^{p^n} = \alpha_i - \alpha_j$$

以及当$\alpha_j \neq 0$时有

$$(\alpha_i \alpha_j^{-1})^{p^n} = \alpha_i^{p^n}(\alpha_j^{p^n})^{-1} = \alpha_i \alpha_j^{-1}$$

所以$\alpha_i - \alpha_j$和$\alpha_i \alpha_j^{-1}$都是$f(x) = x^q - x$的根，即$\alpha_i - \alpha_j$，$\alpha_i \alpha_j^{-1} \in E'$．由此可知$E'$是$E$的子域，而$E'$是由$q = p^n$个元素组成的有限域，其特征数为$p$，故由定理2可知$E'$是$f(x) = x^q - x$在$Z_p$上的分裂域．从而有

$$E' = Z_p(\alpha_1, \alpha_2, \cdots, \alpha_q)$$

故$E = E'$是恰含q个元素的有限域．证完．

最后我们来讨论有限域的结构问题．

定理 4 任一有限域E的非零元素乘法群$\{\dot{E}; \cdot\}$是循环群．

证明 设E的元素个数为q，特征数为p，$(E/Z_p) = n$，则由定理1有$q = p^n$．

由于$\{\dot{E}; \cdot\}$是$h = q - 1$阶群，所以要证它是循环群，则根据命题3，只须证明$\dot{E}$是由Z_p上的所有h次单位根组成的即可．

首先，由$h = p^n - 1$知 $(h, p) = 1$．

其次，$\forall \alpha \in \dot{E}$都有

$$\alpha^h = 1$$

所以$\dot{E}$的每个元素α都是Z_p上的h次单位根．

而$\dot{E}$恰含h个元素，所以$\dot{E}$是E中所有h次单位根组成的集合．于是由命题3，$\{\dot{E}; \cdot\}$是循环群．证完．

由于循环群的结构问题已经解决，所以有限域的乘法群的结构也就清楚了．进一步有重要的

推论 2 任一有限域E都是它所含素域Z_p的单纯代数扩

张。

证明 设E的元素个数为q，则由定理 4，$\dot{E}$是$q-1$阶乘法循环群。设它的生成元为α，于是

$$\dot{E} = (\alpha) = \{\alpha, \alpha^2, \cdots, \alpha^{q-1}\}$$

$$E = \{0, \alpha_1, \alpha^2, \cdots, \alpha^{q-1}\}$$

因此

$$E = \boldsymbol{Z}_p(0, \alpha, \alpha^2, \cdots, \alpha^{q-1}) = \boldsymbol{Z}_p(\alpha)$$

证完。

此推论说明，有限域的结构可以归结为单纯代数扩张的结构，而后者已在 § 3 中解决，所以有限域结构问题的讨论也告完成。

习　　题

1　设E是$q = p^n$个元素的有限域，证明：E中所有非零元之积等于-1（1 的负元）。

2　设α是$\boldsymbol{Z}_p$上的m次不可约多项式$f(x)$的根。则$\alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^m}$都是$f(x)$的根。

3　试造 4 元有限域的加法表和乘法表。

4　证E是特征数为p的有限域，证明：$\forall \alpha \in E$，在E中存在唯一个α的p次方根。

第二部分　近世代数学习指导

本书介绍近世代数的最基本内容：群、环、模和域。

这门课所以叫做“近世代数”，主要是与19世纪以前的代数学相区别。代数学是一门古老的数学学科，19世纪以前，代数学的中心内容是讨论方程式，特别是方程式的求解问题。但是，关于五次方程式的求根公式，在历史上持续很长一段时没有解决。19世纪初叶，法国数学家伽罗瓦（Galos，1811—1832）写了一篇文章《方程式根式可解性条件》，彻底解决了这个问题。他证明，一般的五次方程式不存在用系数的加、减、乘、除、乘方和开方表示的求根公式。伽罗瓦所引入的思想，大大地推动了对于群、域以及其它一些代数体系的研究，使得代数学从新的方向上得到突飞猛进的发展。人们把19世纪以后发展起来的以研究代数体系为内容的代数学叫近世代数学。因为代数体系是建立在抽象集合基础之上的，其中的运算也是抽象的，所以也有人把近世代数叫做抽象代数。

第一章　基本概念学习指导

一　内容概要

本章的主要内容有两个方面：其一是介绍近世代数所用到的集合的一些知识（§1—§3）；其二是概括地讨论代数体系这个基本概念，以及简单介绍几类比群更一般的代数体系：广群、半群和亚群（§4—§6）．通过这一章的学习，可以为进一步研究群、环、模和域打下基础，对近世代数所常用的方法有个初步了解。

二　内容分析

§1　集　　合

（一）内容提要

集合这个概念是康托尔（Cantor,1845—1918）于1894年首先建立的，目前集合的理论已广泛地应用到各个数学分支，成为整个数学的一个基础学科．这一节是介绍集合论中的几个最基本的概念，主要内容有

1　给出集合、元素、子集、空集、集合的交与并、余集、补集、幂集和笛卡尔积集等概念。

2　介绍集合的各种表示方法．主要有两种：列举全部元素表示集合，以及用元素所具有的性质表示集合。

（二）补充说明

1　集合这个概念是数学里的一个“原始概念”，不给精确定义，只做一般性的解释。对集合的解释，目前各种书所用的词汇不全一样，但涵义是一致的，现列举几个，供读者参考：

“数学中讨论的对象叫做元素，若干个或无穷多个元素的集体叫做集合。”

“若干个（有限或无限多个）固定事物的全体叫做一个集合。”

“在一定范围内的讨论对象组成的整体叫做集合”。

2　本书对集合概念的解释是“某一范围内的对象全体叫做集合。”对于这句话，应注意以下几点：

（1）这不是精确定义，因为其中用到的“对象”，“全体”并没有严格定义，不是数学中已定义概念。

（2）这句话里的“对象”是什么都可以，任何东西，任何事物都可以成为我们的观察对象，都可以组成集合。

（3）这句话意味着，一个集合其界限是分明的。也就是说，对于任一集合A和任一元素a，a与A之间的关系必是而且只是下述两种之一：a属于A或者a不属于A，不能含糊不清。比如说“老年人的全体”，这句话便界限不明，无法准确判定每个人是否是老年人，所以不构成我们所讨论的集合。近年来出现一个学科——“模糊集合论”，专门研究这类现象。

（4）一些集合可以做为元素组成一个新的集合，但是任何集合不能是它自身的一个元素，不能说“所有集合的集合”，不能把$\{a\}$与a等同，这会引起逻辑上的矛盾。

3　两个集合的并不能理解为把两个集合并列在一起。例如 $A=\{1,2\}$，$B=\{2,3\}$，则 $A\cup B=\{1,2,3\}$，而不是$A\cup B=\{1,2,2,3\}$。

4　本节中给出许多记号。目前各书所采用的记号不尽相同，同一记号在各书中的涵义也可能不一样。例如，有的书用

$A\subseteq B$表示A是B的子集（A可以不是B的真子集），这相当于我们的记号$A\subseteq B$，而我们用$A\subset B$只表示A是B的真子集。在看参考书时，读者应注意该书对每个记号的解释。

§2 映　　射

（一）内容提要

映射是集合论中的一个非常重要的概念。一般来说，在研究一个集合时，不是只单纯孤立地去观察这个集合的自身，往往要通过这个集合与其它集合之间的联系去了解它的性质。而映射则是体现两个集合之间内在联系的一个重要手段，它是研究集合的不可缺少的工具。映射是读者熟习的函数概念在抽象集合上的推广。这一节介绍映射的概念以及几种特殊类型的映射。主要内容有：

1　给出映射、单射、满射、双射、逆映射、可逆映射、映射合成、变换和置换等概念。

2　讨论映射合成的性质，其中主要的是映射合成满足结合律（定理1）。

3　讨论双射的性质，其中主要是：映射是双射的充分必要条件是这个映射是可逆映射（定理2）。

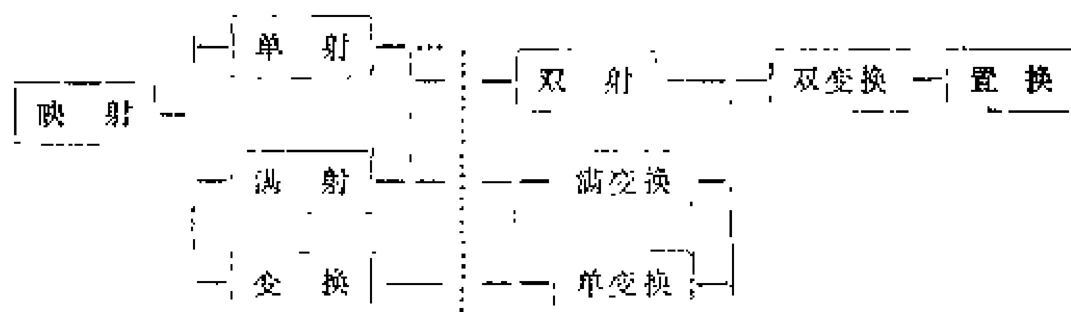
4　介绍变换、特别是置换的一些性质以及置换的表示记号。

（二）补充说明

1　学好本节内容，关键在于对映射定义能正确理解。集合A到集合B的一个法则φ必须满足两个条件才是映射。其一是对A中的每个元素a（一个不漏地）在B中确定一个象a'，其二是对A的每个元素a在B中所确定的象a'必须是唯一的，不能是两个，当然更不能是多个。只具备前一个条件的法则叫做多值映射。例如φ是$\boldsymbol{R}$到$\boldsymbol{C}$的这样法则，它使每个实数a对应a的平方根，则φ是$\boldsymbol{R}$到$\boldsymbol{C}$的一个多值映射。这种多值映射

不是我们现在讨论的对象，我们讨论的映射是单值的。

2　本节讲到的各种映射之间的关系如下图。



3　判定两个映射φ与ψ相等，只须判定两个条件：其一，φ与ψ具有相同的定义域和相同的值域；其二，φ与ψ对定义域里的每个元素a的作用相同，即$\varphi(a)=\psi(a)$。

4　对于双射应给予特殊注意，有时这种映射能比较好地把一个代数体系的代数性质传递到另一个代数体系中去。

定理2从另一个角度刻划了双射。今后判断一个映射φ是双射有两个途径：一个是按定义判定φ是单的而且是满的；另一个是按定理判定φ存在逆映射φ^{-1}。

5　关于“映射”这个名称，有的书叫做“映象”，有的书叫做“写象”，还有的书叫做“函数”。较早几年的书，大都把“满射”叫做“到上的映射”，把“单射”叫做“一一映射”，把“双射”叫做“一一到上的映射”或“一一对应”。

§3　商集与等价关系

（一）内容提要

分类在科学上是一种重要的方法。在这节里，首先对分类所应具备的条件做较详尽的讨论；其次，对在分类过程中起主导作用的等价关系做了介绍；最后论证了做为分类的结果的商集与等价关系的相互依存的性质。

（二）补充说明

1　关于“关系”这个概念，在正文中只做了描述性说

明，没有给出它的精确定义。现把关系的定义列出如下：

设A是任一集合，则$A\times A$的任一子集R叫做A的一个(二元)关系。$\forall a,b\in A$，当$(a,b)\in R$时，则说a对b有关系R，记为aRb.；当$(a,b)\bar{\in} R$时，则说a对b没有关系R，记为$a\bar{R}b$.

2　商集的三个条件，等价关系的三个条件都各是独立的，即不能由其中的任意两条推证其余一条。实际上，无论对于集合的子集族或集合的关系来说，都存在着各种类型的满足其中两条而不满足其余一条的例子。下述“推论”是错误的：“设～是A的一个关系，～具有对称性和传递性，则$\forall a\in A$，取$b\in A$，$a\sim b$。由对称性有$b\sim a$，再由传递性得$a\sim a$。故～具有反身性。”其错误在于“推证”中所取的与a有关系的b不一定存在。上述这段叙述对于解本节习题5有提示作用。

3　设Q是集合A的一个商集，则

$$\nu: a\longmapsto \overline{a}$$

显然是A到Q的满射，叫做A到Q的**自然映射**。关于映射和商集有下述结果。

设φ：$A\longrightarrow B$是满射，则φ决定A的一个商集Q，而且存在唯一的双射$\psi:Q\longrightarrow B$，使得

$$\varphi=\psi\nu$$

其中ν是A到Q的自然映射。

上述结果是后几章中的同态基本定理的雏型，其证明在本章学习指导的例题选讲中给出。

4　做本节习题4、5时，所给出的关系只用记号(例如～)表示就可以，不必说出“～”的涵义，但须对A中的任二元素x，y标明，x对y有还是没有关系～。

§4　代数体系

(一) 内容提要

代数运算、代数体系都是近世代数的基本概念。后几章的

群、环、模和域都是具有一个或两个代数运算的代数体系。研究它们的目的，就是揭示它们各自的代数性质，亦即由它们的代数运算所表现出来的性质。为了顺利达到此目的，有必要先了解代数运算、代数体系这两个概念的涵义。本节就是对这两个概念做介绍，主要内容有：

1　给出三个基本概念：代数运算、代数体系、广群。

2　给出有限集合运算表的构造方法。

3　介绍置换的另一表示方法——表成不相交轮换之积。

（二）补充说明

1　在验证一个法则$\circ$是集合A的运算时，按定义本应验证：$\circ$是$A\times A$到A的一个映射，但在处理具体问题时，可略去映射记号的表述，只要能证明，A的任意两个元素a,b（先后顺序有关）在$\circ$的作用之下得到唯一确定的元素$c\in A$，那么$\circ$就是A的代数运算。大多数场合元素c（运算结果）的存在性和唯一性很容易看出来，但在一个集合的商集中定义运算，运算结果的唯一性一般是不明显的（见例7）。比如在A的商集Q上定义运算$\circ$。$\forall S,T\in Q$，当$a\in S$，$b\in T$时，可用a，b分别做S,T的代表，而记$\overline{a}=S$，$\overline{b}=T$。同样$\forall a'\in S$，$\forall b'\in T$，也可记为$\overline{a'}=S,\overline{b'}=T$。而法则$\circ$又往往是通过代表元素来描述的，此时必须证明$\overline{a}\circ\overline{b}=\overline{a'}\circ\overline{b'}$才能保证$S\circ T$的唯一性。在商集上定义其他映射也有类似现象，需要讨论定义的合理性。

2　对于$\{S_n;\cdot\}$和$\{Z_n;+\cdot\}$应给予特殊注意，它们经常做为例子在后几章中出现。

3　有限集合的运算表的好处是运算结果一目了然，而且从运算表上能看出该运算的一些性质，还可通过造运算表来定义有限集合的运算。

4　注意两个变换（包括置换）ψ，φ的乘积与这两个变换的合成的关系：$\psi\varphi$是ψ与φ的乘积，是φ与ψ的合成，这里

ψ和φ在$\psi\varphi$的两个解释中先后顺序正相反。

§5 同态同构

（一）内容提要

同态、同构是比较两个代数体系性质的重要手段。读者以后会见到，两个同态的代数体系的代数性质有许多是相同的。当我们研究一个代数体系的结构时，如果能够把它与一个结构清楚的代数体系建立同态关系，那么我们便对所研究的这个代数体系的结构有了大致的了解。特别是，如果能够把所研究的代数体系与一个结构清楚的代数体系建立同构关系的话，那么这个代数体系的结构也就完全清楚了。所以寻求建立同态、同构关系是贯穿近世代数始终的一个重要方法。本节只给出这两个概念的定义，至于它们的意义，将在以后的讨论中逐步揭示出来，本节主要内容有：

1　给出两个都具有一个运算的代数体系（广群）之间的同态、单一同态、满同态、同构概念。

2　给出两个都具有n个运算的代数体系之间的同态、单一同态、满同态、同构等概念。

3　介绍同态、同构的简单性质（命题1——命题2）。

（二）补充说明

1　设$\{A;\circ\}$和$\{B;\circ'\}$是两个代数体系，φ是A到B的映射。一般情况如下图

A		B
a	$\xrightarrow{\varphi}$	$\varphi(a)$
b	$\longrightarrow$	$\varphi(b)$
$a\circ b$	$\longrightarrow$	$\varphi(a\circ b)$
$\vdots$		$\varphi(a)\circ'\varphi(b)$
		$\vdots$

其中$\varphi(a\circ b)$和$\varphi(a)\circ'\varphi(b)$一般是$B$中两个不同元素。所谓$\varphi$保持运算，就是$\varphi$保证上述两个元素是同一个元素：$\varphi(a\circ b)=\varphi(a)\circ'\varphi(b)$，也就是说：两个元素（在$\circ$之下）乘积的象恰是这两个元素的象（在$\circ'$之下）的乘积。

2　在证明φ：$A\longrightarrow B$保持运算时，应注意避免出现遗漏现象。对于有限集合，更要特别注意。例如本节习题2，对于所定义的映射φ，在证明$\forall a$，$b\in A$有

$$\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$$

时，a,b应各取遍A的所有元素，$1,i,-1,-i$,漏取一个元素便未完成证明。

3　在上节的学习指导中提到，代数体系的代数性质是"代数运算所表现出来的性质"。当两个代数体系同构时，它们各自由运算所表现出来的性质是完全相同的。所以可以这样说，所谓代数体系的代数性质，就是在同构映射之下保持不变的性质。代数学研究的目标，正是发掘这种性质。

§6　半群　亚群

（一）内容提要

本节简单地介绍两类代数体系：半群和亚群，其目的是为以后研究主要的代数体系做准备。由于半群、亚群的条件较弱，具有更大的普遍性，所以本节所给出的结果在以后各章中均适用。通过这一节的学习，也可初步体验到近世代数的研究手法。本节主要内容有：

1　给出半群、子半群、亚群、子亚群等概念。

2　证明半群的基本性质：广义结合律成立。

3　证明交换半群的基本性质：广义交换律成立。

4　证明半群和亚群的同态象分别是半群和亚群。

（二）补充说明

1　在验证集合A的运算"$\circ$"满足结合律或交换律时，要

避免出现遗漏现象。A是有限集合时更应注意。例如设 $A=\{a,b,c\}$，证明$\forall x,y,z\in A$ 有

$$(x\circ y)\circ z=x\circ(y\circ z)$$

这里需要证明，x,y,z分别取a,b,c中任何元素，等式都成立。当然根据具体情况，有时可以分类，几种可能性可集中一次验证。

2　对于给定集合定义一个运算，要求满足给定条件（如本节习题1，2），可利用定理 3 或定理 4 （或它们的推论），比如习题 1，$A=\{a,b,c\}$是三个元素的集合，$\mathbf{Z}_3$也是三个元素的集合，而且剩余类加法满足结合律。由定理 3 的推论知，所定义的“$\circ_1$”只要使

$$\{\mathbf{Z}_3;+\}\cong\{A;\circ_1\}$$

就可以了。而定义满足这个条件的“$\circ_1$”是不难做到的。

3　从有限集合A的运算表上，能够看出该运算是否满足交换律，A是否具有恒等元。读者应该总结出在上述两种情况下，运算表各有哪些特征。满足结合律的运算表的特征不明显，不必考虑。

4　定理 1 表明，在一个半群A中，任取n个元素 $a_1,a_2,\cdots,a_n$，在排列顺序确定以后，按任何运算顺序做乘法，所得乘积相同。由此，对于给定的n，半群A的乘法便能确定A的一个n元运算

$$(a_1,a_2,\cdots,a_n)\longmapsto a_1,a_2\cdots a_n$$

它是$A\times A\times\cdots\times A$到$A$的映射。

5　例 3 中A无右恒等元的证明如下：设c是非零实数，则

$$\begin{pmatrix}0&c\\0&0\end{pmatrix}\in A$$

对于A的对于的任一元素

$$\begin{pmatrix}x&y\\0&0\end{pmatrix}$$

均有

$$\begin{pmatrix}0 & c\\0 & 0\end{pmatrix}\begin{pmatrix}x & y\\0 & 0\end{pmatrix}=\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}\neq\begin{pmatrix}0 & c\\0 & 0\end{pmatrix}$$

故 A 无右恒等元。类似地可证，B 无左恒等元。

6　以后将看到，在群、环、模、域中，都有与定理 3 以及定理 4 相似的结果。

三　例题选讲

例 1　设 A、B、C 是任意三个集合，证明

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$$

证明　这是集合等式，只须证明等号两端的集合互相包含。

首先，$\forall a\in A\cap(B\cup C)$，由交和并的定义，有 $a\in A$ 并且 $a\in B\cup C$，故 $a\in B$ 或者 $a\in C$。于是有 $a\in A$ 并且 $a\in B$，或者 $a\in A$ 并且 $a\in C$，故 $a\in A\cap B$ 或者 $a\in A\cap C$。从而 $a\in(A\cap B)\cup(A\cap C)$。即

$$A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$$

其次，$\forall b\in(A\cap B)\cup(A\cap C)$，有 $b\in A\cap B$ 或者 $b\in A\cap C$，于是有 $b\in A$ 并且 $b\in B$，或者 $b\in A$ 并且 $b\in C$。由此推得 $b\in A$，并且 $b\in B$ 或者 $b\in C$，故 $b\in B\cup C$，从而 $b\in A\cap(B\cup C)$。即

$$(A\cap B)\cup(A\cap C)\subseteq A\cap(B\cup C)$$

于是由集合相等的定义得到

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$$

例 2　证明，不存在集合 A 到它的幂集 $P(A)$ 的满射。

证明　用反证法。假设存在 A 到 $P(A)$ 的满射 φ，则 $\forall a\in A$ 有 $\varphi(a)\in P(A)$。因 $P(A)$ 是 A 的幂集，所以 $\varphi(a)$ 是 A 的子集。于是必只有以下两者之一成立：$a\in\varphi(a)$ 或者 $a\overline{\in}\varphi(a)$。现令

$$S=\{a\in A\mid a\overline{\in}\varphi(a)\}$$

即 S 是 A 中不属于其（在 φ 之下的）象的元素构成的集合。则 S 在 A 中的补集是

$$S' = \{a \in A \mid a \in \varphi(a)\}$$

即S'是A中属于其（在φ之下的）象的元素构成的集合，显然$A = S \cup S'$，并且$S \cap S' = \phi$。

由于φ是满射，所以$P(A)$的元素S必在A中有原象s

$$\varphi(s) = S$$

对于s也必有下两者之一成立：$s \in S$ 或 $s \bar{\in} S$。但是，当 $s \in S$ 时，由于$S = \varphi(s)$，这与S的构成相矛盾；当$s \bar{\in} S$时，则$s \in S'$，由S'的构成有$s \in \varphi(s) = S$，这与$S \cap S' = \phi$相矛盾。

上述讨论表明，A到$P(A)$的满射φ是不存在的。

例 3 设$\varphi: A \longrightarrow B$是满射，则$\varphi$决定$A$的一个商集$Q$，进而存在唯一的双射$\psi: Q \longrightarrow B$，使得

$$\varphi = \psi v$$

其中v是A到Q的自然映射*。

证明 （一）由φ来确定A的一个商集。$\forall a \in A$，令

$$\overline{a} = \{x \in A \mid \varphi(x) = \varphi(a)\}$$

即$\overline{a}$是A中在φ之下其象与a的象相同的元素所成的子集。容易看出，若$\varphi(a) = \varphi(b)$，则$\overline{a} = \overline{b}$，再令

$$Q = \{\overline{a} \mid a \in A\}$$

则Q便是A的一个商集。事实上

（1）$\forall x \in A$，由于$x \in \overline{x}$，$\overline{x} \in Q$，所以$x \in \bigcup_{\overline{a} \in Q} \overline{a}$，故$A = \bigcup_{\overline{a} \in Q} \overline{a}$。

（2）$\forall \overline{a}, \overline{b} \in Q$。若$\overline{a} \neq \overline{b}$，则$\overline{a} \cap \overline{b} = \phi$。否则存在 $c \in \overline{a} \cap \overline{b}$，于是 $c \in \overline{a}$且 $c \in \overline{b}$。由$\overline{a}$的定义知：$\varphi(c) = \varphi(a)$，$\varphi(c) = \varphi(b)$，从而$\varphi(a) = \varphi(b)$。这表明$\overline{a} = \overline{b}$，与

---

* 关于自然映射的定义，请参阅本章§3学习指导补充说明4。

$\overline{a} \neq \overline{b}$相矛盾，所以$\overline{a} \cap \overline{b} = \phi$。

（3）$\forall \overline{a} \in Q$，因$a \in \overline{a}$，故$\overline{a} \neq \phi$。

（二）证明本题的后一个结论。先定义一个Q到B的映射。$\forall \overline{a} \in Q$，规定

$$\psi: \overline{a} \longmapsto \varphi(a)$$

由于$\overline{a} \in Q$，则有$a \in A$，所以$\varphi(a)$的存在性是显然的。另一方面，当$\overline{b} = \overline{a}$时，由$b \in \overline{a}$有$\varphi(b) = \varphi(a)$。故对$\overline{a}$来说，$\varphi(a)$是唯一的。因此$\psi$是$Q$到$B$的映射。由于$\varphi$是满射，所以$\forall a' \in B$存在$a \in A$，使$\varphi(a) = a'$。于是存在$\overline{a} \in Q$，使$\psi(\overline{a}) = \varphi(a) = a'$。这说明$\psi$是满射。$\forall \overline{a}, \overline{b} \in Q$。$\overline{a} \neq \overline{b}$，则$a \notin \overline{b}$，从而$\varphi(a) \neq \varphi(b)$，即$\psi(\overline{a}) \neq \psi(\overline{b})$，这说明$\psi$是单射。综合上述，$\psi$是$Q$到$B$的双射。

令ν是A到Q的自然映射：$\forall a \in A$有$\nu(a) = \overline{a}$。则

$$\psi\nu(a) = \psi(\nu(a)) = \psi(\overline{a}) = \varphi(a)$$

故

$$\varphi = \psi\nu$$

最后证明，满足此条件的ψ是唯一的。事实上，设τ也是Q到B的双射，而且

$$\varphi = \tau\nu$$

则$\forall \overline{a} \in Q$，由$a \in A$，则有

$$\tau\nu(a) = \varphi(a) = \psi\nu(a),\ \tau(\overline{a}) = \psi(\overline{a}),\ \tau = \psi$$

所以满足上述条件的ψ是唯一的。

例 4　设$A = \{a, b, c, d\}$，乘法如下表

·	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

证明：{A；·}是交换亚群。

证明 1 表的乘积部分的第一行和第一列分别与边行和边列相同，说明 a 是 A 的恒等元。

2 表对于主对角线对称，说明 A 的乘法满足交换律。

3 现在来证明 A 的乘法满足结合律. 首先注意，表的乘积部分的主对角线上的元素都是 a，所以 $\forall x\in A$ 有

$$xx=a$$

下面 $\forall x,y,z\in A$ 证明

$$(xy)z=x(yz)$$

分四种情况讨论。

（1）当 x,y,z 中有恒等元 a 时，显然有

$$(xy)z=x(yz)$$

（2）当 x,y,z 中无 a，而且它们互不相同，由表的右下角三阶方阵可以看出

$$xy=z,\quad yz=x$$

则

$$(xy)z=zz=a,\quad x(yz)=xx=a$$

故

$$(xy)z=x(yz)$$

（3）当 $x=y=z$ 时，则

$$(xy)z=(xx)x=ax=x$$

$$x(yz)=x(xx)=xa=x$$

故

$$x(yz)=(xy)z$$

（4）当x,y,z中无a，而且它们中恰有两个元素相同，此时A中存在$u\neq a,x,y,z$。则　当　$x=y$时有

$$(xy)z=(xx)z=az=z,\quad x(yz)=xu=z$$

当　$x=z$时有

$$(xy)z=uz=y,\quad x(yz)=xu=y$$

当　$y=z$时有

$$(xy)z=uz=x,\quad x(yz)=x(zz)=xa=x$$

总之，此时有

$$(xy)z=x(yz)$$

综上所述，A的乘法满足结合律。　因此$\{A;\cdot\}$是交换亚群。

例 5　对于实数a，规定

$$a_r: x\longmapsto ax,\quad \forall x\in \mathbf{R}$$

再设$\mathbf{R}_r$是所有a_r的集合，即$\mathbf{R}_r=\{a_r|a\in\mathbf{R}\}$。证明：（1）$a_r$是$\mathbf{R}$的变换；（2）$\mathbf{R}_r$关于变换乘法结构成代数体系，而且$\{\mathbf{R}_r;\cdot\}$与$\{\mathbf{R};\cdot\}$同构。

证明（1）$\forall a,\ x\in\mathbf{R}$，因为$ax\in\mathbf{R}$，所以$a_r$是$\mathbf{R}$的变换。

（2）$\forall a_r, b_r\in\mathbf{R}_r$，必有

$$a_r b_r=(ab)_r \qquad (1)$$

事实上，$\forall x\in\mathbf{R}$，有

$$a_r b_r(x)=a_r(b_r(x))=a_r(bx)=abx=(ab)_r(x)$$

（1）式说明，$\mathbf{R}_r$对于变换乘法封闭，所以$\{\mathbf{R}_r;\cdot\}$是广群。现$\forall a\in\mathbf{R}$规定

$$\varphi: a\longmapsto a_r$$

显然φ是$\mathbf{R}$到$\mathbf{R}_r$的双射，而且由（1）式知

$$\varphi(ab)=\varphi(a)\varphi(b)$$

故

$$\varphi:\{\mathbf{R};\cdot\}\simeq\{\mathbf{R}_r;\cdot\}$$

第二章　群学习指导

一　内容概要

群是具有一个代数运算并满足某些条件的比较简单的代数体系。通过这一章的学习使读者初步掌握有关群的最基本知识和研究近世代数最基本的方法。这一章的内容也是学习以后各章的基础。

二　内容分析

§1　群的定义　§2　子群

（一）内容提要

§1、§2 主要给出了群的定义及与定义等价的几个命题；讨论了群的最基本的性质；初步研究了它的子体系——子群及子群的判别条件，介绍一种构造子群的方法，这两节是全章的基础。

（二）补充说明

1 关于群的定义

群是满足特定条件的代数体系。如果给定了一个非空集合G和法则“·”，看G关于“·”能否做成群，首先必须检验“·”是否为G的运算。如果G中任二元素a,b，其积$a\cdot b$仍在G中，即G对“·”封闭，又常说G关于“·”满足闭合律。所以看一个非空集合G关于“·”是否做成群，必须检验下列四条：

（1）闭合律；（2）结合律；（3）恒等元素的存在；（4）逆元素的存在。

这里需要指出的是：结合律是对G中任意三个元素来说的，对于无限群（如第二章§1例6）必须做一般性验证。对于有限群（如第二章§1例7）则需讨论所有可能情形而无遗漏。恒等元是对G的所有元素左乘、右乘都不变的元素，不只是对G的某些元素来说的。这一点在第二章§1定理2的充分性证明中特别重要。逆元素是对每一个元素来说的，应注意的是定义中条件（3）中的e必须是条件（2）中的同一个恒等元。

关于闭合律还需着重指出如下：

如§1例6中的关于“$\circ$”运算封闭，结合律成立，有恒等元为0，但-1无逆元，所以；$\{Q;\circ\}$不是群。去掉-1后，能否立即断言$Q\setminus\{-1\}$关于“$\circ$”运算是群呢？否。尽管群的定义中的（1）、（2）、（3）条对于$Q\{-1\}$显然成立，但“$\circ$”运算对于$Q\setminus\{-1\}$是否封闭并不知道，而这正是$Q\setminus\{-1\}$成群与否的关键，绝不能忽略。现证明如下：

$\forall a,b\in Q\setminus\{-1\}$即，$a\neq -1$，$b\neq -1$。如果

$$a\circ b=a+b+ab=-1$$

则有

$$(1+a)b=-(1+a)$$

因$a\neq -1$，故$1+a\neq 0$，从上式两端消去$1+a$得$b=-1$。这是不可能的。故$a\circ b\neq -1$。即$a\circ b\in Q\setminus\{-1\}$。至此才可断言$Q\setminus\{-1\}$关于“$\circ$”运算做成群。

2　关于群的等价命题

（1）群有多种定义方法，定理1和定理2也可以做为群的定义。除此之外还有其它定义。

（2）定理1中的条件（Ⅰ）、（Ⅱ）比群的定义中的条件（2）、（3）可以说简略了一半，使用起来（如例5）当然是方便的；定理2除可以用来判断一个给定的集合是否是群（如例6），在论证问题中（如定理3的证明）也是很有效的。

3　关于群的等价命题的证明

（1）需要注意的是定理1的（Ⅰ）、（Ⅱ）两条中都突出了一个"左"字，这在充分性的证明中可以看出它的作用。要注意在证明一个元素 a 的左逆元 a' 也是 a 的右逆元时，两个"左"字起了关键性的作用。由于 a 的左逆元 a' 也有左逆元 a''，即有 $a'a=e$，又有 $a''a'=e$，又由于 e 是左恒等元，所以 $aa'=e(aa')=(a''a')(aa')$，再运用结合律就证出了 a 的左逆元也是右逆元，得出 a 有逆元的结论，从而先推得了定义中的条件（3）。而在条件（2）的证明中又用到刚刚证明了的这一结论。

试想，如果将两个"左"字之一换成"右"字，结果又如何呢？请看下例：

设 G 是一个至少有两个元素的非空集合，规定

$$a\circ b=b,\quad \forall a,\ b\in G$$

显然"∘"是 G 的代数运算，并且

$$(a\circ b)\circ c=b\circ c=c,\quad a\circ(b\circ c)=a\circ c=c$$

即运算"∘"满足结合律。

由规定 $a\circ b=b$，显然 G 中任一元皆为左恒等元，且每一元关于给定的左恒等元皆有右逆元，其右逆元即给定的这个左恒等元。但 $\{G;\circ\}$ 显然不是群，因为 $\{G;\circ\}$ 没有右恒等元（当 $a\neq b$ 时）。

如将定理1中条件（Ⅱ）中的"左"字改为"右"，其它不动，其结果怎样呢？请读者自己考虑。

如将定理1中的条件（Ⅰ）、（Ⅱ）中的两个"左"字都换成"右"字，结果又如何呢？请做§1的习题4。

（2）证明定理2的充分性时需要注意的是：在由条件（Ⅰ′）去推（Ⅰ）时，要证 G 有左恒等元 e，证法是：首先取 G 中某一固定（已知）元素 b，由方程

$$yb=b$$

在 G 中有解，取其任一解为 e。这个 e 是对 b 来说满足 $eb=b$

的元素．e 是否为G的左恒等元呢？因为G的左恒等元必须对G的任一元素 a ，均有 $ea=a$ 才行．这一步是不可忽略的．所以还需做进一步的证明，直至证出$ea=a$为止．

4　广群、半群、亚群与群的关系

广群是具有一个代数运算的代数体系的别称，而半群是满足结合律的广群，亚群是有恒等元的半群，群是每一元素都有逆元素的亚群．条件一步步加强，范围则逐渐地缩小．如 $\{\mathbf{Z};\cdot\}$ 是有恒等元素 1 的半群，即亚群，但它不是群．因为不是每一整数都有逆元，而其中只有 ± 1 为可逆元．故 $\{1,-1\}$ 对于整数乘法做成群．又如 $\{M_n(\mathbf{R});\cdot\}$也是有恒等元 E （单位阵）的半群（亚群），但不是群．其中全体可逆阵对于矩阵乘法才做成群（见§1 例3）．所以群是具有更强条件的亚群，是亚群中全体可逆元素做成的．所以我们也可以从半群或亚群出发，加强条件来定义群．

5　关于消去律

我们知道，在群中消去律成立是由于每一元素均有逆元，故若有$ab=ac$，则两端以a^{-1}左乘之，即得$b=c$．但是，消去律成立的代数体系不一定每一元素有逆元．如$\{\mathbf{Z};\cdot\}$中消去律成立，但除± 1外其它元素没有逆元．但对一个有限半群来说，消去律则可充分保证每一元素有逆元（见定理 3 的证明），消去律这个条件则起了重要作用．

一个有限半群如果是群，则消去律成立，从乘法表看，群的全体元素必在每一行，每一列中出现且只出现一次．如果一个有限集合的乘法表不满足上述条件，就可以断定这个集合不作成一个群．如果一个有限半群的乘法表满足上述条件，那么必满足消去律，所以这样的有限半群一定是群，这也可做为判断有限半群是否为群的一种办法．

由群中消去律的成立还可导出一系列结果：如方程$ax=b$，$ya=b$在G中解的唯一性；群和子群的恒等元和逆元素的一致性等，都是利用消去律而得到的．

§ 3 群的同态、同构

（一）内容提要

本节是在第一章初步研究了一般代数体系的同态、同构的基础上，对群这一特定的代数体系做较具体和深入的讨论。并给出有关群的同态、同构的基本性质和对两个群做比较的基本论证方法。这是研究群的构造的重要手段，在§ 4，§ 8 中将会进一步看到它的作用。

（二）补充说明

1　说两个群$\{G;\circ\}$与$\{G';\circ'\}$满同态，简记作$G\overset{\varphi}{\sim}G'$，指的是$\varphi$是$G$到$G'$的满射，且保持运算关系，即

$$\varphi(a\circ b)=\varphi(a)\circ'\varphi(b),\qquad \forall a,b\in G$$

此时，G'一定是G的同态象。

当φ仅仅是G到G'的一个同态映射（不是满射）时，不使用“$G\sim G'$”这个记号。此时，G的同态象$\varphi(G)=\mathrm{im}\varphi\subset G'$。显然$\varphi(G)$是$G'$的一个子群。

2　要证明两个群$\{G;\circ\}$与$\{G';\circ'\}$是同态（同构）的，只需证明存在一个（至少有一个）G到G'的满（双）射，使

$$\varphi(a\circ b)=\varphi(a)\circ'\varphi(b)$$

即可。这种同态（同构）映射可能不止一个。

例如§ 3 中的例 2，$G=\{\boldsymbol{R};+\}$，$G'=\{\boldsymbol{R}^+;\cdot\}$，$\varphi$可以有多种给法，如令

$$\varphi:\quad x\longmapsto a^x,\qquad\qquad a>0\text{的实数}$$

显然φ也是G到G'的同构映射。

在建立这种映射时，必须使G的恒等元e对应着G'的恒等元e'，互相对应着的元素的逆元也互相对应着。一般来说，G的特殊元素必须对应着G'的特殊元素。

3　如果要证明两个群$\{G;\circ\}$与$\{G';\circ'\}$是不同构（不同态）的，则需证明不存在（找不到）G到G'的同构（满同态）

映射．要证明这一点，常需采用反证法，即证明如果有一个同构（满同态）映射存在，使$G\cong G'$（$G\sim G'$），必可导出矛盾．为了导出矛盾，常从特殊元素入手．如例 3 的证明．

4　为了更具体地说明上面2、3两点的意思，再举例如下：

例　$G=\{1, i, -1, -i\}$

$$G_1=\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

$$G_2=\left\{e=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad a=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\quad b=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\right.$$

$$\left.c=\begin{pmatrix}-1&0\\0&1\end{pmatrix}\right\}$$

已知G为 4 次单位根乘群，G_1为以 4 为模剩余类加群 Z_4，由§ 2 习题 5 知G_2关于矩阵乘法作成群．

试问：（1）G与G_1同构否？（2）G与G_2同构否？

列乘法表如下

Ⅰ

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Ⅱ

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Ⅲ

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

（1）令

$$\varphi: 1 \longmapsto \overline{0},\quad i \longmapsto \overline{1},\quad -1 \longmapsto \overline{2},\quad -i \longmapsto \overline{3}$$

显然φ是G到G_1的双射，且在此映射下，表Ⅰ和表Ⅱ完全重合，即φ保持元素间的运算关系不变。故$G \cong G_1$。

（2）如果$G \cong G_2$，必须G的恒等元1对应G_2的恒等元$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$。而$G$中$i$的象必须是$G_2$的$a$，$b$，$c$三个中的一个。不妨令

$$i \longmapsto a$$

则

$$i^2 \longmapsto a^2$$

但$i^2 = -1$，而$a^2 = e$，于是$-1 \longmapsto e$，但$1 \longmapsto e$，则φ不是单射，故φ不是同构映射。同理可证

$$i \longmapsto b \quad 或 \quad i \longmapsto c$$

都会导出同样矛盾。故G与G_2不同构。

学完了§4循环群之后，回答此问题则更简单。因为G和G_1都是4阶循环群，而n阶循环群从同构观点看只有一个，所以$G \cong G_1$。而G_2中的e的阶为1，a，b，c的阶均为2，没有4阶元素，故G_2不是循环群。所以G与G_2不同构。由此易知，若$G \cong G'$，彼此对应着的元素的阶（周期）必须相同（见第二章§4习题14）。

此例说明，尽管G和G_1一个是乘群，一个是加群，但却是

同构的．而G和G_2虽然都是乘群，但却不同构．两个群同构与否与元素的表法及运算符号无关，仅仅取决于它们的代数结构．

5　两个群G与G'同构，只是说G与G'的代数性质完全相同，因而它们有相同的代数结构．我们也常说它们是代数相等的．但同构的群与相同的群是有区别的．如整数加群与所有偶数做成的加群是同构的（§3习题1），但后者是前者的子群．这个例子也说明一个群可以和自己的一个真子群同构．

6　如果群$G\sim G'$，由定理知群G的代数性质完全传递给它的同态象，但反之未必成立．如果$G\cong G'$，则G与G'的代数性质完全相同，这是同态与同构的不同之处．另外，同构映射必须是单射，而同态映射不一定是单射(可以多对一)，这也是两者的区别．虽然群的同态象不象群的同构象那样完全刻划群，但由于它有时比它的原象可能具有某些特殊性及某种便利，研究起来可能比研究原群更容易些．而从一个群的同态象的代数性质又常常可部分地推测原群的性质，所以研究群的同态比研究群的同构来得更灵活一些，运用也更广泛些．

§4　循　环　群

（一）内容提要

本节讨论一类代数结构特别简单的群——循环群．

首先给出这种群的实例（无限的、有限的），然后给出了循环群的定义；接着讨论它的构造，通过定理1（结构定理）证明了：从同构观点看，循环群有且只有两种，并指出它们的代表，解决了循环群的数量和构造问题．其中引进了一个重要的概念——元素的阶；最后又讨论了循环群的子群，解决了循环群的子群的形状、数量等问题，证明了定理2．还讨论了一下循环群的同态象．

从本节的讨论可以初步了解近世代数研究问题的基本方法

和格式。

（二）补充说明

1　关于循环群的构造

循环群的构造定理给出本节最重要的结果。它说明，从同构观点看，循环群只有两个：一个是无限循环群，它与整数加群同构；一个是有限（n 阶）循环群，它与以 n 为模的剩余类加群同构。因此，当需要讨论循环群的某个性质时，我们只要就具体的整数加群和剩余类加群$\{Z_n;\ +\}$讨论即可。

2　关于元素 a 的阶及其重要性质

元素的阶有下述重要性质：如果 a 的阶为 n，那么

（1）$a^m=e\Longleftrightarrow n|m$

（2）$a^{m_1}=a^{m_2}\Longleftrightarrow n\mid m_1-m_2$

如果 a 的阶无限，那么

（3）$a^{m_1}=a^{m_2}\Longleftrightarrow m_1=m_2$。

（1）的证明见§4习题2．（2）、（3）的证明见定理1．在定理1中我们看到，生成元 a 的阶完全决定了循环群的构造。性质（2）、（3）保证了定理中映射 φ 的单射性。元素阶的这些性质在证明中起了关键性的作用。今后还将多次地用到。

3　关于循环群的生成元

循环群的生成元通常不是唯一的。我们有下列重要结果（请见§4 习题9及习题11）。

（1）无限循环群$G=(a)$，有且只有两个生成元 a 与 a^{-1}；

（2）n 阶循环群$G=(a)$，则 a^r是G的生成元当且仅当$(r,n)=1$。

上述结果给出找循环群的生成元的有效方法。

例：$\{Z_9;+\}$的生成元有$\overline{1}$，$\overline{2}$，$\overline{4}$，$\overline{5}$，$\overline{7}$，$\overline{8}$共有6个。

显然 n 阶循环群的生成元的个数等于与 n 互质的正整数的

个数。

4　关于循环群的子群

由定理 2 已将循环群的于群彻底解决。这里需要指出的是“循环群的子群是循环群”，但反之不真。即一个群如果除本身外所有于群都是循环群，这个群本身未必是循环群。例如，克莱茵(Klein) 4 元群 B_4，它的子群（除本身）皆为 1 阶和 2 阶的，故都是循环群，但B_4不是循环群，因为在B_4中没有 4 阶元素。又如例题选讲之例 9 的 4 元数群也是这种群的例子。

5　关于循环群的自同构

由于同构映射必把生成元映成生成元，所以很容易决定循环群的全部自同构。

无限循环群$G=(a)$有且只有两个自同构

$$\varphi_1: a\longmapsto a\ ,\quad \varphi_2: a\longmapsto a$$

n 阶有限循环群的自同构的个数恰等于小于 n 且与 n 互质的正整数的个数。

§ 5　变换群置换群

（一）内容提要

本节主要给出变换群的概念，建立一般抽象群（有限群）和变换群（置换群）之间的重要联系。证明了著名的凯莱定理，指出任何一个抽象群（有限群）都与变换群（置换群）同构，并通过实例加以说明如何去找同构于已知群的变换群。

（二）补充说明

1　关于变换群的概念

我们知道一个集合A的所有变换的集合对于变换乘法并不作成群，其中由双变换作成的群叫做A的变换群。

例如，$A=\{1,2\}$。

$$\tau_1: 1\longmapsto 1,\quad 2\longmapsto 2$$

$$\tau_2: 1\longmapsto 1,\quad 2\longmapsto 1$$

$\tau_3: 1 \longmapsto 2, \quad 2 \longmapsto 2$

$\tau_4: 1 \longmapsto 2, \quad 2 \longmapsto 1$

是A的全部变换．即 $T(A)=\{\tau_1,\tau_2,\tau_3,\tau_4\}$．$T(A)$ 按变换乘法尽管已经构成有恒等元$e=\tau_1$的半群，但对于τ_2来说，不管τ是$T(A)$中那一个变换，都有

$\tau_2\tau: 1 \longmapsto \tau_2(\tau(1))=1, \quad 2 \longmapsto \tau_2(\tau(2))=1$

$\tau_2\tau \neq e=\tau_1$

即τ_2没有逆元，显然τ_2不是双变换．故$T(A)$不作成群．其中τ_1，τ_4是双变换，显然$E(A)=\{\tau_1,\tau_4\}$作成一个群，叫做A的一个变换群．当然仅由$\{\tau_1\}$也作成一个变换群．

在§5习题2中证明了：一个变换群的恒等元一定是恒等变换．§5习题3给出了一个例子．虽然平面π的变换的集合T，对于变换乘法作成了一个群，但它的恒等元不是恒等变换，其中的变换不是由双变换作成的，这样的群不叫变换群．读者不难证明：如果G是集合A的若干个变换所作成的集合，并且G包含恒等变换，若G对于变换乘法作成一个群，那么G只能包含A的双变换．

2　关于凯莱定理

给定了一个群G，G的变换群可能不止一个，但其中有一个和G的关系十分密切，即与G是同构的．这个与G同构的变换群是怎样决定的呢？凯莱定理的证明做出了回答．

定理证明的思路是：先找出一个由G的双变换组成的集合$\overline{G}$，证明$\overline{G}$是群（即变换群）且G与$\overline{G}$同构．

证明的具体方法是：

（1）决定$\overline{G}$．先决定$\overline{G}$的任一元素τ_a．利用G的任一元a按规定可决定G的一个变换τ_a，即把G的任一元x变成ax的变换（左乘变换）．证明τ_a是双变换．于是，给了G一个元，用这种办法就决定了G的一个双变换，把这样得到的所有双变换做成的集合，记作$\overline{G}$．

（2）证明$\overline{G}$是群．首先证明$\overline{G}$对于变换乘法封闭，即$\{\overline{G};\cdot\}$是一个代数体系．接下去本应直接证明$\overline{G}$是一个群（请读者按群的定义证明之），但证明$\overline{G}$是群这一步可以省略．因为只要证得$G\cong\overline{G}$，由G是群$\overline{G}$自然也就是群了．

（3）证明$G\cong\overline{G}$．（这一步包括了（2）的证明）

凯莱定理说明：任一群G都与G上的一个变换群同构．在变换群中总能找到自己的"模型"．把凯莱定理用到有限群上，便得到：任何一个有限群都与一个置换群的子群同构．所以对于变换群（置换群）的研究是有普遍意义的．

例3与例4具体地给出找与一个群同构的变换群的方法．如果所给的群是有限循环群，用例4的方法比例3的方法更简单些．

§6　子群的陪集

（一）内容提要

这一节是在第一章对集合分类的基础上，进一步讨论用子群对群进行分类的问题，并由此得出一些重要结果．本节主要给出子群的陪集、子群的陪集的等价定义，子群在群中的指数等概念，并证明了关于有限群的重要的拉格朗日定理，指出有限群的阶和子群的阶的关系．这一节的学习直接关系着后两节（§7、§8）及其它各章相关部分的学习，所以应给予足够的重视．

（二）补充说明

1　关于子群的陪集的概念

在第一章§3中曾经讨论了对任一集合A进行分类问题，分类的办法可以是很随意的，只要满足分类（构造商集）的三个条件就可以了．本节把对任一集合A分类的思想用于群G，分类的方法不是随意的，而是利用一个子群H作出的．

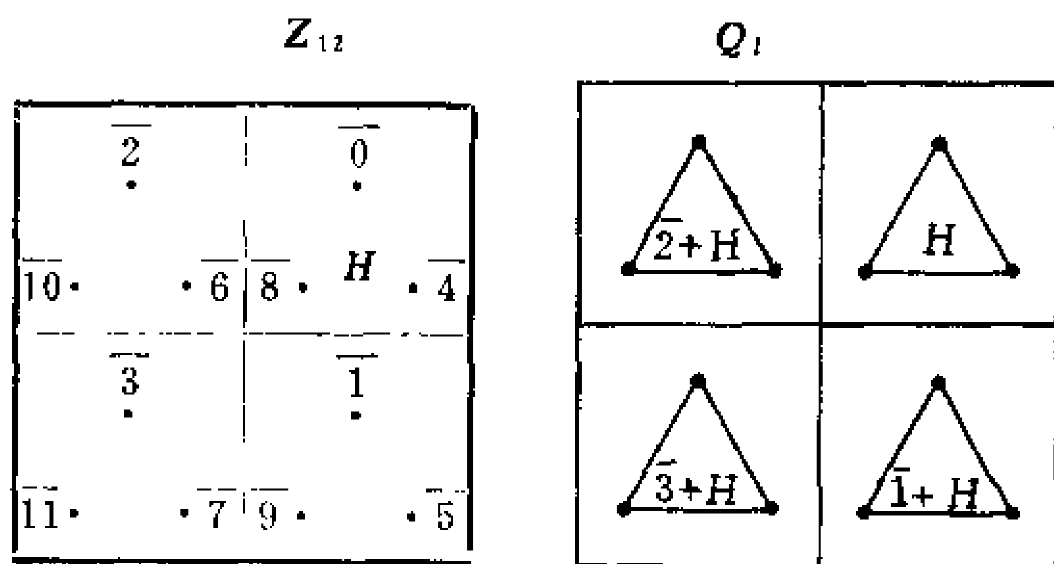
首先定义了群G关于子群H的左（右）陪集的概念（定义1）。通过例2具体地用G的元素a乘子群H的办法求出$G=S_3$关于子群$H=\{(1),(12)\}$的全体左陪集。说明H的全体左陪集做成的集合恰是S_3的一个商集。从而给出了S_3的一个分类，即把S_3的元素以子群H为标准分成了3组（类）。然后通过命题1证明了一般情形。命题1的条件(i)说明全体陪集的并集恰是整个群G；条件(ii)说明两个不同的陪集没有公共元，换句话说，一个元素不可能同时属于不同的两个陪集；条件(iii)说明G的任一元a皆属于某一陪集，每一陪集不空。这3条说明利用群G的子群H所得到的全体陪集恰好给出群G的一个分类，而每一陪集就是一个类。全体陪集做成G关于子群H的一个商集（以陪集为元素的集合）。对于群的研究常常转化为对其关于某子群的商集的研究，这不但是研究群也是研究其它代数体系的一种最基本方法。

以$\boldsymbol{Z}_{12}$为例，在§4习题12中已知$H=\{\overline{0},\overline{4},\overline{8}\}$为$\boldsymbol{Z}_{12}$的一个子群。以$H$为标准，$\boldsymbol{Z}_{12}$的12个元素被分成了4组（类），即4个陪集：

$$H=\{\overline{0},\overline{4},\overline{8}\},\quad \overline{1}+H=\{\overline{1},\overline{5},\overline{9}\}$$
$$\overline{2}+H=\{\overline{2},\overline{6},\overline{10}\},\quad \overline{3}+H=\{\overline{3},\overline{7},\overline{11}\}$$

则 $Q_l=\{H,\overline{1}+H,\overline{2}+H,\overline{3}+H\}$

图示如下



2　关于子群的陪集的等价定义

上面说过利用子群H可以对G进行分类，即得到一个商集，而G的每一个商集都决定一个等价关系．仍以Z_{12}为例．设$\overline{a}$，$\overline{b}\in Z_{12}$，则有

$\overline{a}$，$\overline{b}$在H的同一陪集（类）中$\Longleftrightarrow \overline{b}-\overline{a}\in H$

而后面这个条件$\overline{b}-\overline{a}\in H$．把$Z_{12}$的两个元素是否在$H$的同一陪集（类）中，用子群$H$来衡量的本质特征充分体现出来．所以我们也可以规定关系～如下

$$\overline{a}\sim\overline{b}\Longleftrightarrow\overline{b}-\overline{a}\in H$$

显然关系～是一个等价关系，由此等价关系决定了Z_{12}的一个商集恰是Q_l，而商集Q_l的每一个元素（类）就是Z_{12}关于子群H的一个（左）陪集．

把上述特殊情形推广，对任意群G，利用子群H可定义关系～如下

$$a\sim b\Longleftrightarrow a^{-1}b\in H$$

易证此关系～是一个等价关系．由此等价关系决定G的一个分类，于是得到G的一个商集．这样得到的类就是G关于子群H的左陪集．所以子群H的左陪集也可以这样来定义．这种定义的方便之处是，判断G的两个元素a，b是否属于H的同一陪集，只要看$a^{-1}b$是否属于H就可以了．由本节习题3又知与此条件等价的条件共有6个，都可做为a，b在H的同一个左陪集的判断条件．

3　关于子群H在G中的指数

已有例子（见§6例2）说明，一个群G的子群H的左陪集和右陪集并不一定相同．但定理1的结论说明左商集和右商集之间存在一个双射．即子群H的左陪集和右陪集的“个数”相等．把这个共同的数目叫做子群H在G中的指数．我们看到例2中的子群H在S_3中的指数为3，而例3中的子群H在G中的指数为无限．

定理 1 说明，用子群H来对G分类，不论怎么分，分得的类的数目都相等。命题 2 说明每一类（陪集）中含有的元素数目也一般多，都和H含有的元素个数相等。就是说用子群H，按照我们给出的办法对G分类，分的是很均匀的，不会一类多，一类少。由此自然地导出了重要的拉格朗日定理。

4　关于有限群的阶和子群的阶的关系

拉格朗日定理指出：有限群的子群的阶数必是群的阶数n的约数。但是其逆定理不真。即对群G的阶数n的任一正约数d，G未必有d阶子群。如A_4(S_4中全体偶置换作成的子群—请参考熊全淹的《近世代数》）其阶为12，但却没有 6 阶子群（证明从略）。然而拉格朗日定理的逆定理对于循环群以及有限可换群是成立的。

5　关于定理 1 的证明

在定理 1 的证明中，我们令

$\varphi: aH \longmapsto Ha^{-1}$

是否可以断言φ是左商集Q_l到右商集Q_r的一个映射而不加以证明呢？回答是否定的。因为在φ之下aH的象规定为Ha^{-1}，这个Ha^{-1}由aH的代表a决定。如果$aH=bH$，那么由bH的代表b又决定了bH的象为Hb^{-1}，假如$Ha^{-1}\neq Hb^{-1}$，那么就会出现由于陪集代表选择的不同，同一个陪集所对应的象是不同的，这时φ就不能是一个映射了。所以规定陪集的映射φ时，必须证明在φ之下象与代表的选择无关，亦即说明象是唯一确定的，这一点十分重要。

如果在定理 1 中规定

$\varphi: aH \longmapsto Ha$

行不行呢？φ是不是左商集Q_l到右商集Q_r的映射呢？

以本节例 2 为例：$(13)H=(123)H$，而$H(13)=\{(13),(132)\}$，$H(123)=\{(123),(23)\}$，显然$H(13)\neq H(123)$。

在上面规定的φ之下有

$$(13)H \longmapsto H(13),\qquad (123)H \longmapsto H(123)$$

即同一左陪集由于代表选择的不同，却对应着两个不同的右陪集，因此，上面所规定的φ不是一个映射。

§7　正规子群与商群

（一）内容提要

本节主要讨论一类特殊的重要的子群。给出正规子群的定义、例子、几个等价条件及商群的概念和例子。正规子群和商群对于群的构造的研究具有特殊重要的作用。

（二）补充说明

1　关于正规子群的概念

正规子群是一种特殊的子群，它的特殊性在于它的每一左陪集和相应的右陪集总是相等的。定义中的$aN=Na$的a是对群G中任一元素来说的，而不是对某些a来说的。所以用定义来验证一个子群是不是正规子群必须注意这一点。

还必须注意的是，$aN=Na$指的是用a左乘子群N所得的子集与用a右乘子群N所得的子集是相等的（集合相等），并不是说a可以和N的每一元素可交换。如置换群S_3的子群$K=\{(1),(123),(132)\}$是正规子群

$$(12)K=\{(12),(23),(13)\}$$

$$K(12)=\{(12),(13),(23)\}$$

显然$(12)K=K(12)$，但$(12)(123)=(23)$，而$(123)\cdot(12)=(13)$，元素并不可换。$aN=Na$这个条件相当于对N中任一元素n，必有N中元n'，使$an=n'a$。在证明有关问题和做有关的习题时必须注意到这一点。

一个群G的正规子群的正规子群未必是群G的正规子群。这一点和子群的情形不同（见§7习题9）。

2　关于正规子群的等价条件

用定义来判断一个子群是不是正规子群，就需要验证对G中每一元素a，左陪集aN是否和右陪集Na相等，这有时并不

十分容易．所以我们又给出了和定义等价的另三个条件，即定理的 2)、3)、4)条．因为用条件 4) 只需验证元素ana^{-1}是否在N中，所以有时使用起来比较方便，如例 5 的证明．至于 2)、3)两条除了用来判断一个子群是否为正规子群外，还有更深刻的意义．

在本章例题选讲之例 1 中证明了映射φ_a：$g\longmapsto aga^{-1}$是群G的自同构，叫做G的内自同构．假设φ是群G的自同构，H是群G的子群，如果$\varphi(H)\subseteq H$，我们就说H对φ不变．显然当N是G的正规子群时，$\varphi_a(N)=aNa^{-1}\subseteq N$，即正规子群对内自同构不变．反之，群中对它的所有内自同构都不变的子群就是正规子群．所以正规子群又叫不变子群．

在§2 习题 7 中我们给出了H的共轭子群aHa^{-1}的概念．等价条件2)说明，如果H与它的所有共轭子群aHa^{-1}都相等，那么H就是G的正规子群，反之亦然．

由于共轭子群aHa^{-1}的阶与H的阶相同，所以一个群，如果只有一个阶为n的子群，则此子群必是群G的正规子群（§7 习题 5）．又由例 4 知，指数为 2 的子群必为正规子群．这些都从不同方面提供了正规子群的判断方法．当然上述两个条件只是一个子群是正规子群的充分条件而不是必要条件，在使用时要注意．

3　关于商群的概念

正规子群和商群是紧密联系着的两个概念．由于正规子群的特殊性带来了它的商集的特殊性．这种特殊性不但在于左商集和右商集相同，且可以自然地规定一种运算，使商集G/N做成一个群．这里关键是所规定的运算的合理性．

$$aN\cdot bN=abN$$

如果N仅仅是G的子群，则$aN\cdot bN$未必是一个左陪集．例如，$G=S_3$，$H=\{(1),(12)\}$，已知H不是G的正规子群．

$$(13)H=\{(13),(123)\},\ (23)H=\{(23),(132)\}$$

$$(13)(23)=(132),\ (123)(132)=(1)$$

因$(1)\in(13)H\cdot(23)H$，但$(1)\overline{\in}(13)(23)H$．故$(13)H\cdot(23)H\neq(13)(23)H$．

但当N是G的正规子群时，则有：

$$aN\cdot bN=abN,\qquad \forall a,\ b\in G$$

且这个条件也是充分的（见§7习题4）．因此，在商集G/N中可自然地规定一种运算并使之作成群．

通过例7读者应该学会给了群G的一个正规子群H，如何决定商群．首先需要把H的每一陪集的形状搞清楚，从而决定商群的全部元素，并具体掌握住商群的运算．

4　例6说明有限群的商群G/N一定是有限群，其阶数等于N在G中的指数．但商群的阶为有限的群未必是有限群．如，$G=\{Z;+\}$，$H=(n)$，商群$G/N=\{Z_n;+\}$为n阶有限群，但G为无限群．

5　有限群的每一元素的阶（周期）均有限，但其逆不真．例7就是一个很好的说明．

6　关于群G的两个子群的乘积问题

设A，B是群G的两个子群．一般说来，$AB=\{ab|a\in A,b\in B\}$未必是G的子群．

例如，$G=S_3$，$A=\{(1),(12)\}$，$B=\{(1),(13)\}$．则

$$AB=\{(1),(12),(13),(132)\}$$

由于$(132)\cdot(132)=(123)\overline{\in}AB$，故$AB$不是$S_3$的子群．但是，如果$A$，$B$中有一个是正规子群，情形就不同了．请看§7习题6的证明（见习题解答）．

我们仔细分析一下这个问题的证明关键是什么？“A是正规子群”这个条件在证明中起了什么作用？不难发现，“A是正规子群”这个条件保证了：“对任意的$g\in G$，$a\in A$，存在$a'\in A$，使$ga=a'g$”．这个事实，在证明中起了决定性的作用．其实，我们只要利用“对任意的$x\in B$，$a\in A$，存在，$a'\in A$，使$xa=a'x$”这个条件，就可以证明此问题，甚至再弱一点，只要对任意的$b\in B$，$a\in A$，存在$b'\in B$，$a'\in A$，使$ba=a'b'$成

立就可以了．这样看来，使AB是G的子群，“A是正规子群”这个条件仅仅是充分的，但并不必要．那么，两个子群之积是一个子群的充分必要条件是什么呢？解答请见例题选讲之例2．

§7习题7说明，当A，B，都是G的正规子群，这个加强了的条件，充分保证了AB不仅是G的子群并且是正规子群．

7　关于本节例1符号的说明

在例1中我们使用了如下记号：$G/G=\{G\}$，$G/\{e\}=G$．$G/G=\{G\}$应理解为群G用其正规子群G做分类所得的商集（商群）只含一个元素，即G被分成为一个类$\{G\}$．而$G/\{e\}=G$应理解为群G用正规子群$\{e\}=H$分类所得商集为：$\{aH=a|a\in G\}$即G的每一元素a为一个类（陪集），把它仍记为G．

§8　群的同态基本定理

（一）内容提要

本节主要证明了群论中最重要的定理之一——群的同态基本定理．解决了群G和正规子群N、商群G/N与G的同态象之间的关系．首先给出满同态的核的概念，同时证明了满同态的核是群G的正规子群（命题），然后证明了群的同态基本定理．指出群G的任一商群均是G的同态象（定理1），G的任一同态象从同构观点看，只能是它的商群（定理2）．从本节可以看到，正规子群和商群在研究群的构造中的作用，

（二）补充说明

1　关于满同态的核

G到G'的满同态φ的核N指的是，G中所有在φ之下的象为G'的恒等元e'的元素作成的集合，即e'的完全原象．在命题中证明了φ的核N是G的正规子群．当证明G的一个子集N是满同态φ的核时，一般地必须证明：$N\subseteq\ker\varphi$，且$\ker\varphi\subseteq N$．即需证，$\forall a\in N$，则$\varphi(a)=e'$．即$a\in\ker\varphi$，$N\subseteq\ker\varphi$．反之，$\forall a\in\ker\varphi$，即$\varphi(a)=e'$，往证$a\in N$，$\ker\varphi\subseteq N$．

若$G\overset{\varphi}{\sim}G'$，$\varphi$的核为$N$，由本节习题2知，$G$中任意两个元素$a$，$b$在$G'$中有相同的象的充分必要条件是$a$，$b$在$N$的同一陪集中。即把$G$的元以$N$为标准分类后，$G$中同类元映成$G'$的同一元。核越大，分类越粗，映得的象元就越少，或者说G的这个同态象也就比较"粗糙"。核越小，则分类越细，映得的象元相对前者则较多，这个同态象也就比较"精细"。特别地，当核$N=\{e\}$时，由本节习题4知，此时$G\cong G'$，即G与G'完全等同；当$N=G$时，则$G'=\{e'\}$，整个G映成了一个元。所以同态核N的大小完全刻划了同态映射φ的"精细"程度。

由命题知，同态映射的核必是G的正规子群，由定理1又知，G的任一正规子群N一定是G的某个满同态的核（这个映射就是G到G/N的自然同态）。从这里又进一步揭示了正规子群与一般子群不同的特征，即G的正规子群，且只有这一类子群，才能是这个群的满同态的核。因为G的正规子群N完全决定了商群G/N，从而也就完全决定了G的同态象（定理2），所以作为同态核的正规子群在研究群的构造中处于十分重要的地位。

2　关于定理2的证明

在定理2的证明中，规定

$$\overline{\varphi}: aN\longmapsto a'=\varphi(a)$$

aN在$\overline{\varphi}$之下的象是借助代表元a在φ之下的象来确定的，所以必须首先证明aN的象与代表的选取无关。即证$\overline{\varphi}$是G/N到G'的映射。在证明中我们看到，若$aN=bN$，则$\varphi(a)=\varphi(b)$，即若a，b属于N的同一陪集，则a，b在φ之下的象相同。反之亦然（证明见§8习题2）。这就是说，若$G\sim G'$，把G中元素按象相同与否分类与按同态核N（正规子群）分类实质是一样的。这就决定了G/N与G'之间必然存在双射$\overline{\varphi}$，而且$\overline{\varphi}$是

同构映射。

3　关于三个群G，G'，G/N的关系，此处$G\overset{\varphi}{\sim}G'$，$N$是满同态映射$\varphi$的核。

（1）$G\overset{\varphi}{\sim}G'$其核为$N$，$N$为$G$的正规子群；

（2）$G\overset{\nu}{\sim}G/N$，ν为自然同态（定理1）；

（3）$G/N\overset{\overline{\varphi}}{\cong}G'$（定理2）

三个映射φ、ν、$\overline{\varphi}$又是什么关系呢？

由于

$$\varphi: a \overset{\nu}{\longmapsto} aN \overset{\overline{\varphi}}{\longmapsto} a' = \varphi(a)$$

所以有：$\varphi = \overline{\varphi}\nu$（或直接验证）。

上述关系说明，G的任一商群都是G的同态象，G的任一同态象（从同构观点看）也只能是它的商群。所以，G的同态象只须从它的商群里找。而G的商群完全由G和G的正规子群N所决定。因此，只要掌握了G的所有正规子群即掌握了G的所有商群，从而也就掌握了G的所有同态象。显然G有多少正规子群就有多少同态映射，正规子群和同态映射是一一对应的。但正规子群和G的同态象（不同构的）之间可能不是一一对应的，因为可能由G的几个不同的正规子群（如例题选讲例9中的H_2，H_3,H_4）都得到同一商群(Z_2)，但是由正规子群却能够决定G的所有同态象。从这里读者可以很好体会同态基本定理的深刻含意及正规子群与商群的重要作用（以§8的例2及习题7和例题选讲例9为例理解之）。

4　在§8习题9中，已知$G\overset{\varphi}{\sim}G'$，$A'$是$G'$的所有子群的集合，而$A$则是$G$中包含$\ker\varphi=K$的子群$H$的集合。该题证明$A$与$A'$之间存在双射。这里$H\supseteq K$这个条件在证明中起什么

作用呢？没有这个条件结论还对不对呢？只要细心分析不难发现，$H\supseteq K$ 这个条件保证了 φ 的单射性. 若没有这个条件，则结论不能成立。

试看一例. 已知$\{Z;+\}\sim\{Z_6;+\}$，其核为Z的子群 $K=(6)$. Z_6有且只有4个子群

$H_1'=\{\overline{0}\}$，$H_2'=\{\overline{0},\overline{3}\}$，$H_3'=\{\overline{0},\overline{2},\overline{4}\}$，$H_4'=Z_6$.但$\{Z;+\}$却有无限多个子群.显然两个群的子群的集合之间不存在双射. 事实上，$\{Z;+\}$的子群（2），（4）的象相同，都是H_3'（其实$\{Z;+\}$中有无穷多个子群的象都是H'_3，请读者考虑一下还有哪一些）. 而在$\{Z;+\}$中包含核$K=(6)$的子群只有 4 个

$$H_1=K=(6),\ H_2=(3),H_3=(2),H_4=Z=(1)$$

（注意：这些子群的生成元都是 6 的约数）.

在$A=\{H_1, H_2, H_3, H_4\}$ 和 $A'=\{H_1', H_2', H_3', H_4'\}$之间确实存在双射 φ：$H_i\longmapsto H_i'=\varphi(H_i)\ (i=1,2,3,4)$). 从这个例子看到，“$H\supseteq K$” 这个条件的作用是绝对不可忽视的. 假如没有这个条件，不但上面的结论不再成立，题中的后一个结论也不再成立。

例如，取$G=S_3$，$G'=\{1,-1\}$（乘群）. 设φ是把 S_3 中的偶置换映成G'的恒等元 1，把奇置换映成 -1 的映射，易知 φ是G到G'的满同态映射，即$G\overset{\varphi}{\sim}G'$. 又知$H=\{(1),(12)\}$是$S_3$的子群，但不是$S_3$的正规子群. 但$\varphi(H)=G'$是$G'$的正规子群. 这是由于$H$不包含$\ker\varphi=\{(1),(123),(132)\}$的缘故.

在 § 8 的另一些习题中（如第 3 题，第10 题）也有“$H\supseteq K$”这个条件，请读者注意在这些问题的证明中这个条件的作用.

5　对于 n 阶有限群G来说，其任一同态象的阶必等于某一商群G/N的阶，而G/N的阶恰为N在G中的指数，由拉格朗日定理知G/N的阶为G的阶的约数，从而G的任一同态象的阶也必为G的阶的约数. 由此可知12阶群决不会和 5 阶群同态，

4 阶群决不会和 3 阶群同态．但对于G的阶数n的任一正约数d，是否一定存在d阶群作为G的同态象呢？G需具备什么条件结论才对呢？（请参考 § 8 习题8）

§ 9 直　和

（一）内容提要

直和是群论中一个重要概念，它给出如何用几个群去合成（构造）一个群，使合成的群具有与原群同构的子群；也给出一个群如何分解成几个子群的合成，用以考虑该群的结构．本节主要介绍如下几个问题：

1　加群的（外）直和概念；

2　加群（外）直和的基本性质；

3　加群分解成子群的和，与加群分解成子群的（内）直和等概念．

（二）补充说明

1　这里仅就加群讨论了（内）直和与（外）直和的概念．对一般的群我们也可以定义（外）直积（群的运算为乘法）和（内）直积，原则上不存在任何困难，就可以把直和的结果推广到直积上．

2　正文中列举的例子是各具特点的，读者应仔细体会．

3　习题 2 说明了（内）直和与(外)直和的联系，读者可将此题推广成一般性的一个定理．

4　（内）直和与（外）直和讲义中均取同一记号“$\oplus$”，这是因为在代数观点下，（内）直和也可以看作是（外）直和，可以认为是等同的．

三　例题选讲

例 1　假设a是群G的一元，那么映射

$$\varphi_a: g \longmapsto aga^{-1} \qquad \forall g \in G$$

是G的自同构。称φ_a为G的内自同构。

证明　先证φ_a为G到自身的双射。$\forall g \in G$，显然有G的元$a^{-1}ga$，使

$$a^{-1}ga \longmapsto a(a^{-1}ga)a^{-1} = g$$

即$g = \varphi(a^{-1}ga)$。故φ_a为G的满射。

又$\forall h \in G$　有

$$h \longmapsto aha^{-1}$$

如果$aga^{-1} = aha^{-1}$，那么$g = h$。所以φ_a是G的单射。从而φ_a为G到自身的双射。

再证φ_a保持运算。由于

$$\varphi_a(gh) = a(gh)a^{-1} = aga^{-1} \cdot aha^{-1} = \varphi_a(g) \cdot \varphi_a(h)$$

因此φ_a为G的自同构。

例2　设A，B是群G的子群，则AB是G的子群的充分必要条件是$AB = BA$。

证明　必要性　假如AB是G的子群，$\forall ba \in BA, a \in A, b \in B$。因为$A$和$B$都是$G$的子群，所以$a^{-1} \in A$，$b^{-1} \in B$。因为$ba = (a^{-1}b^{-1})^{-1}$，而$a^{-1}b^{-1} \in AB$，$AB$是$G$的子群，所以，$(a^{-1}b^{-1})^{-1} \in AB$，从而有：$ba \in AB$。所以，$BA \subseteq AB$。

同理可证，$\forall ab \in AB$必有$ab \in BA$，即$AB \subseteq BA$。综合上述得到：$AB = BA$。

充分性　假如$AB = BA$(集合相等)。$\forall ab \in AB$；存在$a' \in A$，$b' \in B$，使$ab = b'a'$。于是$\forall a_1b_1, a_2b_2 \in AB$，有

$$(a_1b_1)(a_2b_2) = a_1(b_1a_2)b_2 = a_1(a_2'b'_1)b_2$$
$$= (a_1a_2')(b_1'b_2) \in AB$$

故AB对G的运算封闭。

又　$(ab)^{-1} = b^{-1}a^{-1} = a''b'' \in AB$

从而AB为G的子群。

证明此题要注意，$AB = BA$，并不是元素可交换，而是集合A和B可交换，即集合AB与BA相等。所以对于A，B中任意元

a，b，不一定有$ab=ba$，一般只能有$ab=b'a'$，$ba=a''b''$。这里$a',a''\in A$，$b',b''\in B$。当G是可换群时，显然$AB=BA$。此命题自然成立.

例 3　设a，b为群G中两个元素，且$ab=ba$，a 的阶为m，b 的阶为n，则ab的阶为m，n的最小公倍数$q=[m,n]$的约数，且群G中含有阶为q的元。

证明　分两种情形

（1）若$(m,n)=1$，见§4习题7。

（2）若$(m,n)\neq 1$，设

$$m=P_1^{\alpha_1}P_2^{\alpha_2}\cdots P_t^{\alpha_t}P_{t+1}^{\alpha_{t+1}}\cdots P_s^{\alpha_s}$$

$$n=P_1^{\beta_1}P_2^{\beta_2}\cdots P_t^{\beta_t}P_{t+1}^{\beta_{t+1}}\cdots P_s^{\beta_s}$$

不妨设$\alpha_1\leqslant\beta_1$，$\alpha_2\leqslant\beta_2$，…，$\alpha_t\leqslant\beta_t$；$\alpha_{t+1}\geqslant\beta_{t+1}$，…，$\alpha_s\geqslant\beta_s$ $(1\leqslant t\leqslant s)$。则$m$，$n$的最小公倍数

$$q=[m,n]=P_1^{\beta_1}P_2^{\beta_2}\cdots P_t^{\beta_t}P_{t+1}^{\alpha_{t+1}}\cdots P_s^{\alpha_s}$$

因为a的阶为m，b的阶为n，故$a^{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}}$的阶为$m_1=P_{t+1}^{\alpha_{t+1}}P_{t+2}^{\alpha_{t+2}}\cdots P_s^{\alpha_s}$，$b^{p_{t+1}^{\beta_{t+1}}p_{t+2}^{\beta_{t+2}}\cdots p_s^{\beta_s}}$的阶为$n_1=P_1^{\beta_1}P_2^{\beta_2}\cdots P_t^{\beta_t}$因$(m_1,n_1)=1$，故由(1)$a^{p_1^{\alpha_1}\cdots p_t^{\alpha_t}}\cdot b^{p_{t+1}^{\beta_{t+1}}\cdots p_s^{\beta_s}}$的阶为$m_1n_1=q$。

又由

$$(ab)^q=(a^{n_1})^{m_1}\cdot(b^{m_1})^{n_1}=(a^{(p_1^{\alpha_1}\cdots p_t^{\alpha_t})l})^{m_1}$$

$$\cdot(b^{(p_{t+1}^{\beta_{t+1}}\cdots p_s^{\beta_s})k})^{n_1}$$

$$=(a^m)^l\cdot(b^n)^k=e^l\cdot e^k=e$$

故ab的阶是$q=[m,n]$的约数.（见学习指导§4补充说明2(1)）

其中$l=P_1^{\beta_1-\alpha_1}P_2^{\beta_2-\alpha_2}\cdots P_t^{\beta_t-\alpha_t}$，$k=P_{t+1}^{\alpha_{t+1}-\beta_{t+1}}\cdots P_s^{\alpha_s-\beta_s}$。

注意：若$ab\neq ba$，此结论未必成立。例如，令$G=GL_3(R)$

（见§1例3），取

$$a=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix},\quad b=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$$

$ab\neq ba$，a与b的阶皆为2。但$(ab)^2\neq e$，事实上ab的阶为3。

例 4　假如可换群G中阶为有限的元的最大阶数为m，试证：G中阶为有限的任意元的阶都是m的约数。

证明　用反证法。若G中有某元b的阶为n，但$n\nmid m$。则由上例知存在阶为$q=[m, n]$的元素c，而$q>m$。这与G中元的最大阶数为m矛盾。

例 5　设$H_1=(a^s)$，$H_2=(a^t)$是循环群$G=(a)$的两个子群，证明：$H_1\cap H_2=(a^d)$，此处d是s，t的最小公倍数，记作$d=[s, t]$。

证　若s，t至少有一个为0，结论显然成立。若s，t均不为0，由于$H_1\cap H_2$是G的子群且为循环群，因此$H_1\cap H_2=(a^k)$。下面证明$H_1\cap H_2=(a^d)$。因$d=[s, t]$，则有$d=sr_1=tr_2$，且$(r_1,r_2)=1$。因而有$a^d=(a^s)^{r_1}=(a^t)^{r_2}$，从而$a^d\in H_1\cap H_2$，所以$(a^d)\subseteq H_1\cap H_2$。又因$a^k\in H_1\cap H_2$，有

$$a^k=(a^s)^{k_1}=(a^t)^{k_2},\quad k_1,\ k_2\in Z \qquad (※)$$

下面分两种情形讨论。

（1）若a的阶为无限，则由（※）式有，$k=sk_1=tk_2$ $\Longrightarrow d\mid k\Longrightarrow a^k\in(a^d)\Longrightarrow H_1\cap H_2=(a^k)\subseteq(a^d)$。故$H_1\cap H_2=(a^d)$。

（2）若a的阶为n，由（※）式有，$n\mid k-sk_1$，$n\mid k-tk_2$ $\Longrightarrow n\mid r_1(k-sk_1)$，$n\mid r_2(k-tk_2)$。

因　$(r_1,r_2)=1$，所以存在$u,v\in Z$，使$r_1u+r_2v=1$。于是又有$n\mid u(r_1k-dk_1)$，$n\mid v(r_2k-dk_2)\Longrightarrow k(r_1u+r_2v)-d(k_1u+k_2v)=nq$，即$k-d(k_1u+k_2v)=nq$

所以$a^k=a^{d(k_1u+k_2v)}\in(a^d)$从而有：$(a^k)=H_1\cap H_2\subseteq(a^d)$。故$H_1\cap H_2=(a^d)$。

综上讨论可知，$H_1\cap H_2=(a^d)$。

例 6　证明，阶数为pq（p，q为互异素数）的可换群必为循环群。

证　证明的基本想法是：如果能证出群G中一定存在阶为pq的元素，那么G必是循环群。下面就设法找出阶为pq的元。

因为G为pq阶可换群。由§7习题12知G中至少有一个阶为p或q的元。不妨设a为G中阶为p的元。令$H=(a)$，则H是G的p阶正规子群，从而商群G/H是q阶群。因q为素数，故G/H是循环群。设G/H的生成元为bH。那么$(bH)^q=b^qH=H$，于是推出$b^q\in H$。可以断言，b的阶不能是p，因为由$b^p=e\in H$，$b^q\in H$，且$(p,q)=1$，则存在整数s，t使$ps+qt=1$。于是

$$b=b^{ps+qt}=(b^p)^s\cdot(b^q)^t\in H$$

与$b\bar{\in}H$矛盾（显然$bH\neq H$）。因此，b的阶只能是pq或q（元素的阶是群的阶的约数）。若b的阶为pq，则$G=(b)$为循环群；若b的阶为q，则ab的阶为pq，$G=(ab)$也为循环群。

此例说明，6阶、10阶、14阶、15阶、21阶…有限可换群必是循环群。

例 7　如果$p<q$都是素数，证明：pq阶群的q阶子群必是正规子群。

证明　证明的基本思路是：如果能够证明G中q阶子群只能有一个，则由§7习题5的结论知，q阶子群必为正规子群。

用反证法。若G中有两个不同的q阶子群H_1，H_2。因$H_1\cap H_2$也是H_1，H_2的子群，其阶数整除q。因q为素数，故$H_1\cap H_2$的阶只能是1和q。显然$H_1\cap H_2$的阶不能是q，否则$H_1\cap H_2=H_1=H_2$，与$H_1\neq H_2$矛盾。故$H_1\cap H_2=\{e\}$。看G的子集

$$H_1H_2=\{h_1h_2|h_1\in H_1,\ h_2\in H_2\}$$

可证H_1H_2恰含q^2个元素。这是因为若$h_1h_2=h_1'h_2'$，$h_1'\in H_1$，$h_2'\in H_2$。那么$(h_1')^{-1}h_1=h_2'h_2^{-1}\in H_1\cap H_2=\{e\}$。故$(h_1')^{-1}h_1$

$=h_2'h_2^{-1}=e$，即$h_1=h_1'$，$h_2=h_2'$．所以，H_1H_2 中有 q^2 个元．但 $H_1H_2\subseteq G$．这与G的阶为$pq<q^2$ 矛盾．从而证明了G中不可能有两个不同的 q 阶子群．即若N为G的 q 阶子群，则必唯一，故由 § 7 习题 5 N为正规子群．

例 8　证明：就同构意义来说，6 阶群只有两个，一个是循环群，一个是 S_3．

证明　设G为 6 阶群，$a\in G$，$a\neq e$，则 a 的阶只能是2，3，6．

（1）当G含有阶为 6 的元素时，显然G为循环群；

（2）当G不含阶为 6 的元素时，则$G\cong S_3$．

因为，G中除 e 外，元素的阶不能都是 2．不然，若元素的阶均为 2，则G为交换群，由例 6 知，6 阶交换群必为循环群．这与G不含阶为 6 的元矛盾．故G中至少有一个元素 a 的阶为 3．于是$H=\{e,a,a^2\}$为G的 3 阶子群．由例 7 的证明知，$6=2\times 3$，6阶群最多只有一个3阶子群．所以H是G的唯一的3阶子群，且是正规子群．取$b\in G$，但$b\notin H$，则 $b\neq e$，b 的阶只能是 2．不然 b 的阶必是 3，则(b)是异于H的 3 阶子群，矛盾．于是$G=H\cup Hb=\{e,a,a^2,b,ab,a^2b\}$．由$H$为正规子群，有$bH=Hb$．故$ba\in Hb=\{b,ab,a^2b\}$．

若$ba=b$，则$a=e$，与 a 的阶为 3 矛盾．

若$ba=ab$，则ab的阶为 6（因 a 与 b 的阶互素），此与G不含阶为 6 的元矛盾．故只有$ba=a^2b$．利用这个关系式，可决定G的乘法表，例如

$$ba^2=(ba)a=(a^2b)a=a^2(ba)=a^2(a^2b)=ab$$

$$b(ab)=(ba)b=a^2b^2=a^2$$

$$(ab)a=a(ba)=a(a^2b)=b$$

$$(ab)(ab)=a(ba)b=a(a^2b)b=a^3b^2=e$$

$$(ab)(a^2b)=a(ba^2)b=a(ab)b=a^2,\ \cdots$$

可得G的乘法表为

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

令φ： $e\longmapsto(1)$， $a\longmapsto(123)$， $a^2\longmapsto(132)$，

$b\longmapsto(12)$， $ab\longmapsto(13)$， $a^2b\longmapsto(23)$

则G与S_3的乘法表重合，故φ是G到S_3的一个同构映射。于是$G\cong S_3$。

例 9 设G含有 8 个元素

$$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \pm\begin{pmatrix}i&0\\0&-i\end{pmatrix},\quad \pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad \pm\begin{pmatrix}0&i\\i&0\end{pmatrix},$$

$(i^2=-1)$

证明：G关于矩阵乘法构成一个非交换群，G的每个子群都是正规子群。并决定G的所有同态象。

证明 令

$$e=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad a_1=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\quad a_2=\begin{pmatrix}i&0\\0&-i\end{pmatrix},$$

$$a_3=\begin{pmatrix}-i&0\\0&i\end{pmatrix},\quad a_4=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad a_5=\begin{pmatrix}0&-1\\1&0\end{pmatrix},$$

$$a_6=\begin{pmatrix}0&i\\i&0\end{pmatrix},\quad a_7=\begin{pmatrix}0&-i\\-i&0\end{pmatrix}.$$

G的乘法表为

	e	a_1	a_2	a_3	a_4	a_5	a_6	a_7
e	e	a_1	a_2	a_3	a_4	a_5	a_6	a_7
a_1	a_1	e	a_3	a_2	a_5	a_4	a_7	a_6
a_2	a_2	a_3	a_1	e	a_6	a_7	a_5	a_4
a_3	a_3	a_2	e	a_1	a_7	a_6	a_4	a_5
a_4	a_4	a_5	a_7	a_6	a_1	e	a_2	a_3
a_5	a_5	a_4	a_6	a_7	e	a_1	a_3	a_2
a_6	a_6	a_7	a_4	a_5	a_3	a_2	a_1	e
a_7	a_7	a_6	a_5	a_4	a_2	a_3	e	a_1

由乘法表可见G关于矩阵乘法封闭．显然G的乘法满足结合律，于是$\{G;\ \cdot\}$是有限半群．又G中每一元都在表的各行、各列出现且只出现一次，故G中乘法满足消去律，故$\{G;\ \cdot\}$是一个群．此群叫 4 元数群．由表显然G不是交换群．

因G为 8 阶群，由拉格朗日定理知，它的子群的阶数只能是1, 2, 4, 8．而 2 阶子群必为循环群，只能由阶为 2 的元生成．G中阶为 2 的元只有一个a_1，故 2 阶子群只有一个为：$H_1=\{e, a_1\}$．G中除e，a_1外其余各元的阶皆为 4．故G的 4 阶子群皆为循环群，共有 3 个为：

$$H_2=(a_2)=(a_3)=\{e, a_1, a_2, a_3\}$$

$$H_3=(a_4)=(a_5)=\{e, a_1, a_4, a_5\}$$

$$H_4=(a_6)=(a_7)=\{e, a_1, a_6, a_7\}$$

（由有限群的子群的判别条件 3，从表上看运算封闭的子集也只有以上 3 个）．

下面证明G的所有子群皆为正规子群．

因为 2 阶子群H_1中的元为纯量阵，显然和G的任一元可交

换，即$\forall g\in G$，$gH_1=H_1g$，故H_1为G的正规子群（或利用§7习题5的结论）．

因为4阶子群的指数为2，故为正规子群．另外，$\{e\}$，G显然是G的正规子群．故G的所有子群皆为正规子群．这样的群又叫汉弥尔顿(Hamilton)群．

其相应的商群为

$$G/\{e\}=G,\qquad G/G=\{G\}\cong\{e\}$$

$G/H_1=\{H_1,\ a_2H_1, a_4H_1, a_6H_1\}$，因$G/H_1$中除恒等元$H_1$外，其余各元的阶皆为2，故$G/H_1\cong B_4$．

$G/H_2=\{H_2, a_4H_2\}$（其中$a_4H_2=\{a_4, a_5, a_6, a_7\}$）为2阶群，故为循环群．由于2阶群从同构观点看只有一个，故

$$G/H_2\cong G/H_3\cong G/H_4\cong Z_2$$

由此例可以看出，四元数群共有6个正规子群，从而决定了6个商群，由本章§8定理1知，这6个商群都是G的同态象，又由§8定理2知，G的任一同态象必与它的一个商群同构，而G的不同构的商群只有4个，所以，G的同态象（不同构的）也只有4个，即

$$G,\ \{e\},\ B_4,\ Z_2$$

例10 设N是G的正规子群，K是G的子群，证明，$K\cap N$是K的正规子群，并且

$$K/(K\cap N)\cong KN/N$$

证明 如果能够证明$K\sim KN/N$，且同态核为$K\cap N$，则知$K\cap N$为K的正规子群，于是由同态基本定理即得证．下面来作证明．

因N是G的正规子群，$N\subseteq KN$，故N也是G的子群KN的正规子群，所以KN/N有意义．且KN/N的每一元均具有形式kN．$k\in K$．

先证明$K\sim KN/N$．$\forall k\in K$，则$kN\in KN/N$，且kN由k唯一决定．令

$$\varphi: k\longmapsto kN,\quad \forall k\in K$$

则 φ 是 K 到KN/N的映射. 由于KN/N的每一元均具形式kN，故 φ 是 K 到KN/N的满射.

又 $\forall k_1, k_2 \in K$，有

$$\varphi(k_1k_2) = k_1k_2N = k_1N \cdot k_2N = \varphi(k_1)\varphi(k_2)$$

故 φ 是 K 到KN/N的满同态。从而

$$K \sim KN/N$$

最后证明 φ 的核是$N \cap K$。因为

$$\ker\varphi = \{k \mid k \in K, \varphi(k) = N\}$$

$\forall x \in K \cap N$，$\varphi(x) = xN = N$(因$x \in N$)，故$x \in \ker\varphi$。即$K \cap N \subseteq \ker\varphi$。另一方面，$\forall x \in \ker\varphi$，则$\varphi(x) = xN = N$，即 $x \in N$，又$x \in K$，于是$x \in K \cap N$。即$\ker\varphi \subseteq K \cap N$。故$K \cap N = \ker\varphi$。由 § 8 命题知$K \cap N$为 K 的正规子群，再由同态基本定理可知

$$K/K \cap N \cong KN/N$$

此题也可以先证明$K \cap N$是 K 的正规子群，则$K/K \cap N$有意义。再令

$$\varphi: k(K \cap N) \longmapsto kN$$

证明 φ 是$K/K \cap N$到KN/N的同构映射。请读者试证之。

第三章　环与域学习指导

一　内容概要

本章的主要内容是介绍有两个代数运算的特殊的代数体系，环和域。

环的原始模型是整数环 $\mathbf{Z}$，对于整数环来说，关于加法和乘法，$\{\mathbf{Z}; +\}$和$\{\mathbf{Z}; \cdot\}$分别是加群和半群，讨论整数环时是同时讨论这两个代数体系，并把它们通过分配律联系起来。

环论与群论不同，群论的背景从本质上来说只有一个，来源于变换群，而环论却是从许多专门理论当中汇合起来的。所以与群论相比，环论显得不那么整齐和统一。

但是，我们将会从大量的实例中体会到，环论这个分支的丰富内容和重要性。在下一章，我们将会看到，类似于产生变换群的方式同样产生环，就是加群的自同态环。

本章首先介绍环的定义和例子，然后介绍一些特殊类型的环：交换环、有单位元的环、整环、除环和域，然后研究子环、理想、商环和同态这些基本概念。它们分别类似于群论中的子群、正规子群、商群和同态。本章的后半部分，侧重于有单位元的交换环的讨论：首先研究它们的某些“扩张”，介绍没有真零因子的交换环的商域和极大理想，讨论一元多项式环的构成和性质，在本章最后，介绍整环的因子分解的基本理论。

二 内容分析

§1—§3 环的定义，整环、除环和域、子环

（一）内容提要

§1—§3给出了本章中一些基本概念。§1给出了环的定义和例子，并讨论了环的一些基本性质。因为当$\{R;+,\cdot\}$是环时，则要求$\{R;+\}$和$\{R;\cdot\}$分别是加群和乘法半群，所以，环R具备加群和乘法半群所具有的一切性质。又因为，当R是环时，则加群$\{R;+\}$和半群$\{R;\cdot\}$这两个代数体系是通过分配律发生联系的。由此，进一步导出了环R的下述性质

（1）$0a=a0=0$

（2）$(-a)b=a(-b)=-ab$

（3）$(-a)(-b)=ab$，$\forall a,b\in R$

在§1又介绍了单位元和可逆元（单位）的概念。

§2介绍具有某些特殊性质的环。为此首先引进了零因子的定义，然后在此基础上，引进了整环、除环与域的定义。

§3　给出了子环（体、域）的定义以及子环（体、域）的判定条件。

在§1—§3中所举出的例子是很重要的。在以后各节进一步讨论环时，还将多次用到这些例子。这些例子是

（1）整数环$\mathbf{Z}$、偶数环、有理数域Q、实数域R、复数域C、实数域R上的多项式环$R[x]$。上述的每一个都是交换环，而且都没有真零因子。除偶数环外，每个环都有单位元；

（2）实数域R上的全阵环$M_n(R)$，它是一个有单位元的非交换环$(n>1)$，而且含有真零因子；

（3）$[0,1]$上的所有实函数所构成的环是一个含无限个

元的交换环，它含真零因子；

（4）四元数除环K．它是一个含无限个元的有单位元的非交换环，而且每个非零元都是可逆元，即是一个非交换的除环；

（5）$\mathbf{Z}_n$——以n为模的剩余类环．它是一个含有限个元、有单位元的交换环．当$n=p$是素数时，$\mathbf{Z}_p$是域．当n是合数时，$\mathbf{Z}_n$有真零因子．

在上述所举例子中，稍细心一点就会发现，还缺少一个含有限个元的非交换环例子．我们在下一节就可以举出这样的例子．

（二）补充说明

1　关于单位元

对于环R来说，它可能有单位元，也可能没有单位元．例如，整数环$\mathbf{Z}$有单位元，但偶数环没有单位元．

就环R与其子环S来说，可能

（1）R有单位元但S没有单位元（把偶数环看作整数环$\mathbf{Z}$的子环时，$\mathbf{Z}$有单位元，偶数数环没有单位元）；

（2）R没有单位元但S有单位元（§3例6）；

（3）R和S都有单位元，但两个单位元不相同（§3例5、例6）；

（4）R和S都有单位元，它们的单位元相同（§3例2）．

2　关于可逆元（单位）

可逆元（单位）的概念只是对有1的环才有意义．以后也常把可逆元说成单位．请读者务必注意，单位与单位元是有区别的：

（1）若环R及其子环S都有单位元，而且相同时，如果a是S中的可逆元则a也必是R中的可逆元，而且a在S中的逆元与a在R中的逆元是一致的．反之，若a是R中的可逆元，则当$a\in S$时未必a也是S的可逆元．例如，整数环$\mathbf{Z}$是有

理数域Q的子环，它们有相同的单位元。因为Q是域，所以任意非零元都是Q的可逆元。但是，$\mathbf{Z}$中可逆元只有± 1，显然$\mathbf{Z}$中任意$a\neq \pm 1,0$在Q中是Q的可逆元，但在$\mathbf{Z}$中a不是$\mathbf{Z}$的可逆元。

（2）环R没有单位元，R的子环S有单位元时，如果$a\in S$是S的可逆元，则因R没有单位元，所以不能说a是否是R的可逆元（参看§3例6中的R与S）。至于S没有单位元，而R有单位元时，当然也不能谈S中的元素a是否是S的可逆元。例如，偶数环是一个没有单位元的环，它是有理数域Q的子环。Q中非零偶数都是Q的可逆元，但因偶数环没有单位元，所以在偶数环中谈不上非零偶数是否是偶数环的可逆元。

（3）当环R及其子环都有单位元，但它们的单位元不相同时，从§3例5的剩余类环$\mathbf{Z}_6$及其子环S_1和S_2的关系，以及§3例6中的$M_2(C)$和S的关系可以看出，子环S的可逆元a在其扩环R中不是R的可逆元。

例如，例5中的S_1以及S_2中各自的非零元，分别在S_1和S_2中都是可逆元，但S_1和S_2的非零元在$\mathbf{Z}_6$中都是真零因子，所以S_1和S_2的可逆元不是$\mathbf{Z}_6$的可逆元；对例6中的$M_2(C)$的子环S来说，S中的任意非零元都是$M_2(C)$的真零因子，自然S中的可逆元也不能是$M_2(C)$的可逆元。

通过上述对§3例5、例6的分析，我们自然会提出如下的问题：

当环R及其子环S都有单位元，但二者不同时，那么S中的可逆元a是否一定不是R的可逆元？或者说，R的可逆元是否一定不能在S中？

关于这个问题，答案是肯定的，

即，环R及其子环S有不同的单位元时，如果$a(\in S)$在S中是可逆元，则a在R中不能是R的可逆元。现证明如下：

设1和$1'$分别是R和S的单位元，且$1\neq 1'$，$a\in S$是S的

可逆元。往证：a 不是 R 的可逆元。用反证法。若 a 是 R 的可逆元，则 a 不能是 R 的真零因子。这时，因为

$$a = 1 \cdot a = 1' \cdot a$$

有

$$1 \cdot a - 1' \cdot a = 0, \text{ 即 } (1 - 1')a = 0$$

因 a 不能是 R 的真零因子，所以

$$1 - 1' = 0, \text{ 即 } 1 = 1'$$

与 $1 \neq 1'$ 矛盾。

所以，a 不能是 R 的可逆元。

由上面的证明可以看出，R 的可逆元绝不能在 S 中（R 与 S 的单位元不相同时）。

3　关于零因子

若 S 是环 R 的子环，$a \in S$ 是 S 的零因子。显然 a 也是 R 的零因子；若 a 不是 S 的零因子，则 a 未必一定不是 R 的零因子。这一点从§3的例5和例6即可看出。

4　关于整环的定义

本书关于整环 I 的定义，要求 I 是有1没有真零因子的交换环。但有的书把有1没有真零因子的环叫做整环。请读者在阅读参考书和有关材料时，要注意该处关于整环的定义是否要求具有交换性。

5　关于环的类型

（1）按环 R 所含元的个数是否有限分为有限环和无限环；

（2）按环 R 的乘法是否满足交换律可分为交换环和非交换环；

（3）按环 R 是否有单位元分为有1的环和没有1的环；

（4）按环 R 是否有真零因子分为含真零因子的环和不含真零因子的环。有1没有真零因子的交换环叫做整环；

（5）当 $\{R;\cdot\}$ 是乘群时，则称环 R 为除环。交换除环叫做域。

§4 矩 阵 环

（一）内容提要

在高等代数中，我们对数域上的矩阵和行列式是很熟习的。为了以后讨论的需要，本节对它们作了推广，给出了任意环R上的矩阵和交换环R上的n阶方阵A的行列式的定义。并进一步给出：

1　环R上的全体n阶方阵的集合$M_n(R)$关于矩阵的加法和乘法构成一个环。

2　矩阵A的行列式$detA$可按行（或列）展开

$$\begin{aligned}\det A&=a_{i1}A_{i1}+a_{i2}A_{i2}+\cdots+a_{in}A_{in}\\&=a_{1j}A_{1j}+a_{2j}A_{2j}+\cdots+a_{nj}A_{nj},\quad i,j=1,2,\cdots,n\end{aligned}$$

而且

$$a_{i1}A_{j1}+a_{i2}A_{j2}+\cdots+a_{in}A_{jn}=0$$
$$a_{1i}A_{1j}+a_{2i}A_{2j}+\cdots+a_{ni}A_{nj}=0,\quad i\neq j$$

其中，A_{ij}是A中元素a_{ij}在A中的代数余子式。

3　$\det(AB)=(\det A)(\det B)$

4　$A\tilde{A}=\tilde{A}A=(\det A)E_n$

其中$\tilde{A}$是A的伴随阵。

5　有1的交换R上的n阶方阵A有逆阵必要而且只要$\det A$是R的可逆元（单位）。

6　当F为域时，$A\in M_n(F)$，A有逆阵必要而且只要$\det A\neq 0$。

7　R是有1的交换环，$A,B\in M_n(R)$，若$AB=E_n$，则$B=A^{-1}$。于是有$BA=E_n$。

上述结果，是高等代数中对数域上的n阶方阵和行列式的相应结果的推广。

（二）补充说明

1　本节所给出的行列式的定义是对有1的交换环R上的n阶方阵给出的．对R是除环时（非交换）也可以定义R上的n阶方阵的行列式，但稍复杂些．

2　在本节给出了矩阵单位的定义．正文中已指出，矩阵单位不是全阵环$M_n(R)(n>1)$的单位（可逆元），矩阵单位都是真零因子．

§5　理想与商环（差环）

（一）内容提要

理想在研究环的理论中，与群论中的正规子群的作用很类似．本节首先介绍了（左、右、双边）理想的定义，以及环R的子集N是（左、右、双边）理想的判定条件．然后，给出了一种构造环R的理想的方法，并在此基础上给出了主理想和主理想环的定义．最后，关于环R对理想N的商集R/N，引进了加法和乘法，并证明$\{R;+,\cdot\}$是一个环．

（二）补充说明

1　关于理想和商集 R/N的运算

在第二章群论中，我们看到当N是群G的正规子群时，则可对商集G/N定义运算

$$(xN)\cdot(yN)=(xy)N,\quad \forall x,\ y\in G$$

使$\{G/N;\cdot\}$是群，称G/N为G关于N的商群．

对于环R来说，从群的角度看，$\{R;+\}$是加群，R的任一子环N是R的子群．因为加群的子群都是正规子群，所以R关于子环N有商群，姑且也记作 R/N．这时，$R/N=\{x+N|x\in R\}$．

从环的角度来说，环是有两个代数运算的代数体系．所以，自然地会提出下面的问题：

由环R的加法能对R/N定义加法使R/N构成加群，那么能否通过R的乘法，再给 R/N 定义一个乘法而使R/N是一个环

呢？

这个问题，对研究环的理论来说应该说是很自然的。我们知道，通过环R的加法给R/N所定义的加法，是按下面的方式规定

$$(x+N)+(y+N)=(x+y)+N,\quad \forall x,\ y\in R$$

那么，对环R的乘法来说，要想通过它再给R/N定义一个乘法，我们很自然地会想到应该按下面的方式去定义

$$(x+N)\cdot(y+N)=xy+N,\quad \forall x,\ y\in R$$

但是，上述的规定一般来说，不能保证一定是R/N的一个代数运算。由于商集R/N是由子环N确定的，所以为保证上述规定的合理性，必须对子环N附加一些条件。那么，子环N具备什么条件，才能保证上述规定是R/N的代数运算呢？

根据代数运算的定义，要保证

$$(x+N)\cdot(y+N)=xy+N$$

是R/N的代数运算，必须保证$xy+N$是由$x+N$和$y+N$所确定的R/N中的唯一确定的元素。显然$xy+N\in R/N$，但是，$xy+N$是与$x+N$和$y+N$的表法有关。而在R/N中，只要$x-x'\in N$，则$x+N=x'+N$。所以，要保证上述规定是R/N的代数运算，必须保证上述规定与$x+N$的代表x选取无关才行。亦即若$x+N=x'+N, y+N=y'+N$时，必须$xy+N=x'y'+N$，即$xy-x'y'\in N$才行。

我们知道，当$x+N=x'+N$，$y+N=y'+N$时，则有$x-x'$，$y-y'\in N$。从而有

$$x=x'+n_1,\quad y=y'+n_2,\quad n_1,n_2\in N$$

这时

$$xy=(x'+n_1)(y'+n_2)=x'y'+x'n_2+n_1y'+n_1n_2$$

所以，$xy-x'y'=x'n_2+n_1y'+n_1n_2$。

为了保证$xy-x'y'\in N$，从上式可以看出，N只须满足条件

$$\forall n\in N,\ r\in R\ \Rightarrow nr,\ rn\in N$$

这样就引出了理想的定义．本节在引出理想定义之前，先一般地给出了左、右理想的定义．

当N是环R的理想时，则商集R/N就可以借助R的加法和乘法，定义出R/N的加法和乘法．由于R/N的加法和乘法是由R/N中的元 $x+N$ 的代表x，通过R的加法和乘法确定的，所以R/N的加法和乘法也满足R的加法和乘法所满足的算律．

2　关于本节中的例子

例1指出，任意环R一定有平凡（当然）理想；例5指出，域只有平凡（当然）理想，不能再有其它理想，这一结论对除环也对；例2说明 $N=(m)$是整数环$\mathbf{Z}$的理想，而且N是$\mathbf{Z}$的主理想（例6），例8进一步说明$\mathbf{Z}$是主理想环；例3说明：$N=\{f(x)\in F[x]\mid f(1)=0\}$是$F[x]$的理想．由例3容易看出：$\overline{N}=\{f(x)\in F[x]\mid f(c)=0$，$c$是$F$中确定的数$\}$也是$F(x)$的理想；例7说明例3中的理想$N$是 $F[x]$ 的主理想，而且N是由$x-1$生成的，即$N=(x-1)$．

请读者想一想，上述的$\overline{N}$是否是 $F[x]$的主理想？如果是，$\overline{N}$是$F[x]$中哪个元生成的？

类似整数环是主理想环的证明，可以证明数域F上的多项式环$F[x]$也是主理想环．

例9和例10给出了两个商环的例子，前者是 $\mathbf{Z}_n$，后者是由如下四个元：$0+N$，$1+N$，$i+N$，$(1+i)+N$组成．例9很重要．请读者要很好的掌握．

例4给出一个由环R中n个元：$a_1,a_2,\cdots,a_n$构造R的一个左理想的方法．

3　关于主理想

从主理想的定义可以看出，主理想是环R的一类构造既简单又容易掌握的理想．特别是，当R是有1的交换环时，则(a)的构造更为简单，很象整数环 $\mathbf{Z}$中的理想(a)，由R中一切形如na的元构成，其中n为任意整数．我们知道主理想环是一个整环，而且它的任一理想都是主理想．所以，主理想环比起一

般环来，构造一定容易掌握。

§6　环的同态与同态基本定理

（一）内容提要

上节对环R的理想N，证明了R对N的商集 R/N 是一个环。由于商环R/N的两个运算是通过R的加法和乘法确定的，所以找出R及其商环之间的联系是很自然的。事实上，第二章研究群及其商群之间的联系，也正是在上述想法之下进行的。

本节首先在有两个代数运算的代数体系之间的同态与同构概念的基础上，对环明确了环的同态与同构的含义，进一步指出了环的同态与同构的一些性质；随后证明了在环的理论中占有重要地位的环的同态基本定理；最后对环的同态与同构给出了一些结果。

（二）补充说明

1　关于环的同态基本定理

环的同态基本定理的意义与群的同态基本定理完全类似。它说明：环R的任一商环R/N都是R的同态象，而环R的任一同态象从同构的观点看只能是R的商环。

因此，由环R的任一理想N都可得到R的一个同态象。反之，由R的任一同态象都能得到R的一个理想（即满同态的核）。

另一方面，我们知道作为环R的同态象 R'来说，R'未必与R具有完全相同的性质。但是，通过环的同态基本定理可知，在R中一定存在一个理想（即满同态的核）使得R' 与R/N具有完全相同的性质。因此，只要掌握了 R/N 就掌握了R的同态象R'。

综合上述，可以看出理想与商环的重要作用。

2　关于定理 3

定理 3 说明，当环$\overline{S}$与环R的子环S同构，而且$\overline{S}$与S在R中的补集S'没有公共元时，那么从同构的观点，$\overline{S}$可以看成

环R的子环。

定理 3 叫做挖补定理，这种称呼从定理的证明过程去看是很自然的。

证明定理时，我们由$R=\{x_1,\ y_1,\ \cdots|x,\ y,\cdots\}$先确定了一个$\overline{R}=\{\overline{x_1},\overline{y_1},\ \cdots|x,\ y,\ \cdots\}$。事实上，$\overline{R}$就是$\overline{S}$和$S'$的并集：$\overline{S}\cup S'$，也可以说，从$R$中把$S$挖出来，然后再把$\overline{S}$补进去所得到的集合就是$\overline{R}$。由于题设规定$\overline{S}$与$S$的补集没有公共元，所以$\overline{R}$才能写为：$\overline{R}=\{\overline{x}_1,\ \overline{y}_1,\ \cdots|x,\ y,\cdots\}$的形式，从而为规定$R$到$\overline{R}$的双射提供了可能性。

应用定理3，可以把一个没有单位元的环嵌入到一个有单位元的环中去。

§ 7　极大理想与素理想

（一）内容提要

在本节给出了极大理想和素理想的定义，并进一步给出由一个交换环得到域的方法：R是有 1 的交换环．R/N是域$\Longleftrightarrow$ N是R的极大理想（定理 1）．

关于素理想给出了：N是环R的理想．N是环R的素理想$\Longleftrightarrow R/N$没有真零因子（定理 2）．在有 1 的交换环中，极大理想必为素理想（推论）．上述推论在本章 § 11将看到它的应用。

（二）补充说明

1　关于极大理想的定义

关于极大理想，本书将环R本身排除在外，有些书则不是这样，其定义如下．

如果环R的理想N在R中除自身和R外，不再有包含N的理想，则称N为R的极大理想。

按上述定义，环R本身是R的极大理想．但按本书的定义，环R不是R的极大理想。

由于极大理想的定义有差别，所以涉及极大理想的有关结论，请读者注意该结论中关于极大理想的定义条件。

2　关于定理 1

本节定理 1 指出：N是有 1 的交换环R的理想。R/N是域$\Longleftrightarrow N$是R的极大理想。

从定理必要性的证明中，可以看出R有单位元的条件并没用到。所以，定理 1 的必要性对任意交换环都成立。即：R是交换环，若R/N是域，则N是R的极大理想。

但是，我们看到在定理充分性的证明中，用到了R有单位元的条件。那么，对任意交换环来说，有否可能用其它方法证出定理的充分性呢？亦即，对任意交换环R来说，当N是R的极大理想时，R/N是否一定是域？

答案是否定的。例如对偶数环R来说，(4)是R的极大理想。这是因为，若令N是R的理想，而且$N\supset(4)$时，则在N中必有 $a\in N$，但$a\notin(4)$。由此可知a是偶数但不是 4 的倍数。于是a与 4 的最大公因数为 2，所以由整数的性质知，存在两个整数s和t，使

$$4s+at=2$$

上式说明$2\in N$，所以有 $N=R$。即 (4)是R的极大理想。但 $R/(4)$不是域。这是因为，$2\notin(4)$，所以$2+(4)$不是 $R/(4)$中的零元。然而，$\{2+(4)\}\cdot\{2+(4)\}=2\cdot 2+(4)=4+(4)$ 是$R/(4)$中的零元，即$2+(4)$是 $R/(4)$的真零因子。故 $R/(4)$不能是域。

上面所提到的偶数环是没有单位元的交换环，所以上例说明，定理 1 的充分性必须在R是有 1 的交换环的情形才成立。

3　关于素理想的定义

关于素理想，1949年麦柯(McCoy)给出了如下的定义：

若N是环R的理想，对环R中任意两个理想A和B，如果$AB\subseteq N$，则$A\subseteq N$或$B\subseteq N$，则称理想N为R的素理想。

当R是交换环时，如果N是环R的素理想(按上述定义)，

由$ab\in N$则有$(a)(b)\subseteq N$，于是由素理想定义，则有$(a)\subseteq N$或$(b)\subseteq N$。从而有$a\in N$或$b\in N$。因此，本书中的素理想是上述定义的特例。

4　关于本节的推论

定理2的推论指出：有1的交换环R的极大理想必是素理想。

但是，对于没有1的交换环来说，极大理想未必一定是素理想。

例如，补充说明2中所举的例，（4）是偶数环R的极大理想，而$R/(4)$有真零因子。所以根据本节定理2知（4）不是R的素理想。

§9　多项式环　§10　整环和域上的多项式环

（一）内容提要

在§9给出有1的交换环R上未定元x的多项式的定义，然后证明了未定元存在定理。在§10主要介绍整环和域上的多项式的一些进一步结果。这些结果主要有：

1　整环I上的多项式环$I[x]$是整环（§10定理1）；

2　带余除法（定理2）及其推论（推论2）；

3　余式定理（定理3）；

4　多项式的根与整除性（推论3）；

5　c是$f(x)$的重根$\Longleftrightarrow x-c\mid f(x),f'(x)$（定理4）；

6　域F上的多项式环$F[x]$是主理想环（定理5）；

7　域F上的多项式环$F[x]$的因子分解定理（定理8）。

（二）补充说明

1　关于多项式环

在高等代数中，我们曾把形如

$$a_0+a_1x+\cdots+a_nx^n \tag{*}$$

的式子叫做数域F上的多项式。其中，$a_i\in F$，n为任意非负

整数．对于多项式，规定了相等以及加法和乘法．但是，在当时并没有说明这一表示式的确切意义，表示式中所出现的很多符号是不清楚的．例如，x 是什么？在没有定义运算之前，在表示式(*)中所出现的符号“+”和“·”是什么意思？

又如，我们常对多项式变更写法，按照未知量降幂去排列是否合理？如果说，表示式(*)只是一种形式的写法，那么其中所出现的符号“+”是否满足交换律？

因此，根据上面所提出的一些问题，确定多项式的构造是必要的。

在§9我们以有1的交换环为“系数域”，确定了多项式环的构造，证明了未定元的存在性．这样一来，上面所提出的一些问题自然都解决了．

2　关于多项式函数

高等代数讨论多项式时，曾指出：可以把多项式 $f(x)$ 看作未知量 x 的函数，x 取数域 F 中的任意数．这种看法的重要依据是，多项式按表法是否完全一致所定义的相等，与函数的相等是一致的。

但是，对于任意有1的交换环 I 上的多项式 $f(x)$，我们不能采用函数的观点去处理．这是因为，当 I 是有限环时，例如，取 $I=\mathbf{Z}_2=\{\overline{0},\ \overline{1}\}$．这时，$I[x]$ 中的多项式：$f(x)=x+\overline{1}$ 和 $g(x)=x^2+\overline{1}$ 是不相等的两个多项式．但是，$f(x)$ 和 $g(x)$ 在 $x=\overline{0}$ 的值都等于 $\overline{1}$，在 $x=\overline{1}$ 时的值都等于 $\overline{0}$．而 $I=\mathbf{Z}_2$ 只含 $\overline{0}$ 和 $\overline{1}$ 这两个元。所以，作为变数 x 的函数 $f(x)$ 和 $g(x)$ 是相等的。因此，对于任意有1交换环 I，不能把多项式看作 x 的函数。

3　关于整环与域上的多项式环的一些结果

§10对整环与域上的多项式环给出了一些结果，这些结果与高等代数中数域上多项式环的相应结果是相同的。只不过在整环情形，对个别结果加上了某些限制．这些结果的证明基本上与数域上多项式环的证明是相同的，只有定理6的证明有差

别。

本书处理多项式的因子分解理论时，没有引进最大公因子的概念，其实，定理 6 中所出现的$d(x)$就是$f(x)$与$g(x)$的最大公因子。而定理 6 所给出的结果就是：多项式$f(x)$与$g(x)$的最大公因子 $d(x)$可表为 $f(x)$与$g(x)$的倍式和：$f(x)u(x)+g(x)v(x)=d(x)$。

由于带余除法基本定理在域 F 上的多项式环$F[x]$中成立，所以，高等代数中有关整除性和最大公因子的结果和方法，完全可以毫不变动地拿到$F[x]$中来。

4　关于定理 3

定理 3 指出：$R[x_1,x_2,\cdots,x_n]\sim R[\alpha_1,\alpha_2,\cdots,\alpha_n]$，所以

$$\forall f_1(x_1,x_2,\cdots,x_n),f_2(x_1,x_2,\cdots,x_n)\in R[x_1,x_2,\cdots,x_n]$$

若

$$F(x_1,x_2,\cdots,x_n)=f_1(x_1,x_2,\cdots,x_n)f_2(x_1,x_2,\cdots,x_n)$$

则有

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=f_1(\alpha_1,\alpha_2,\cdots,\alpha_n)f_2(\alpha_1,\alpha_2,\cdots,\alpha_n)$$

上述关系说明用α_i代x_i的可能，这是普通多项式的一个重要性质。

5　关于多项式环$R[\alpha]$和$R[\alpha_1,\alpha_2,\cdots,\alpha_n]$

通常，环 R 上的 n 元多项式 $f(x_1,x_2,\cdots,x_n)$ 总是指 $f(x_1,x_2,\cdots,x_n)$是 R 上的无关未定元 $x_1,x_2,\cdots,x_n$的多项式。所以，当 α 不是 R 上的未定元，$\alpha_1,\alpha_2,\cdots,\alpha_n$ 不是 R 上的无关未定元时，则$f(\alpha)$和$f(\alpha_1,\alpha_2,\cdots,\alpha_n)$不是 F 上的多项式。

在本书中，为了叙述方便借用了多项式的叫法，也把$f(\alpha)$和$f(\alpha_1,\alpha_2,\cdots,\alpha_n)$称为 R 上的多项式。

§11　唯一分解环

（一）内容提要

本章开始时曾提出：整数环是环的一个重要的原始模型。

我们知道，对整数环中任意不等于± 1的非0整数来说，都能分解为有限个素数之积，而且不计次序和± 1的因子差别，分解是唯一的。一般称此结果为唯一分解定理。

本节将对一般整环讨论整除性的初等理论，指出在主理想环中唯一分解定理成立。为了讨论一般整环的整除性，本节对整环给出了整除、因子、倍元、相伴元以及素元等概念。关于整环的整除性的研究，本节重点放在主理想环。对主理想环证明了：主理想环是唯一分解环。随后指出欧氏环是主理想环，从而欧氏环也是唯一分解环。本节最后，给出了唯一分解环的一个重要性质：唯一分解环中任意n个元：$a_1,a_2,\cdots,a_n$一定有最大公因子。

（二）补充说明

1　关于素元

素元的定义可以看作整数环中素数的推广，但是，素数有一个很重要的性质：

（1）若$p|ab$，则$p|a$或$p|b$。

性质（1）对任意整环来说，并不一定成立。例如，本节例4指出整环

$$I=\{a+b\sqrt{-3}\,|\,a,b\in Z\}$$

不是唯一分解环。在讨论中，我们看到I中的元4，分解为素元之积的形式有两种

$$4=2\cdot 2=(1+\sqrt{-3})(1-\sqrt{-3}) \qquad (*)$$

其中，2，$1+\sqrt{-3}$，$1-\sqrt{-3}$都是I的素元，而且$1+\sqrt{-3}$和$1-\sqrt{-3}$都不是2的相伴元。由（*）式可以看出，$2|(1+\sqrt{-3})(1-\sqrt{-3})$。因为2，$1+\sqrt{-3}$，$1-\sqrt{-3}$都是$I$的素元，而且$1+\sqrt{-3}$和$1-\sqrt{-3}$都不是2的相伴元。所以，2不能整除$1+\sqrt{-3}$，也不能整除$1+\sqrt{-3}$。

但是，对于唯一分解环来说，一定具有性质（1）。事实上，设p为唯一分解环I的素元，如果

$p|ab$，往证 $p|a$ 或 $p|b$。

因为 I 是唯一分解环，所以，a 和 b 在 I 中有唯一分解：

$$a = p_1p_2\cdots p_s,\quad b = q_1q_2\cdots q_t$$

其中 p_i 和 q_j 都是素元。于是

$$ab = p_1p_2\cdots p_sq_1q_2\cdots q_t$$

另一方面，因为 $p|ab$，所以有

$$ab = pq = pq'_1q'_2\cdots q'_r$$，其中 q'_i 是素元。

于是

$$ab = p_1p_2\cdots p_sq_1q_2\cdots q_t = pq'_1q'_2\cdots q'_r$$

因为，I 是唯一分解环，所以，p 必与某一 p_i 或某一 q_j 相伴。若 p 与 p_i 相伴，则 $p|a$，若 p 与 q_j 相伴，则 $p|b$。

综上所述，可知唯一分解环的素元一定具有性质（1）。反之，一个整环的每一素元都具有性质（1）时，则能保证分解的唯一性。这一点从整数环或主理想环中唯一分解定理成立的唯一性证明中，都能看到上述结论是正确的，当然，这并不是说，整环如果具有性质（1）就是唯一分解环。这是因为性质（1）并不能保证整环中的每个元都能分解为素元之积。

2　关于整环 I 中非可逆的非0元可分解为素元之积的条件

本节定理 2 证明 I 中非可逆元 $a(\neq 0)$ 可以分解为素元之积时，用到了主理想环的一个重要性质：

（2）I 中任意真因子序列

$$a_1, a_2, \cdots, a_n, \cdots$$

只能含有有限项。其中，$a_{i+1}|a_i$，$i = 1, 2, \cdots$。

事实上，对于唯一分解环来说，具有性质（2）是显然的，而且，从定理 2 的证明中可以看出，正是主理想环具有性质（2），才保证了非可逆元 $a(\neq 0)$ 可分解为素元之积。

因此，一个整环 I 如果具有性质（2），则 I 中任意非可逆元 $a(\neq 0)$，一定都可分解为素元之积。

3　整环 I 是唯一分解环的充要条件

通过上述可知

I 是唯一分解环$\Longleftrightarrow I$ 具有性质（1）和（2）。

三 例题选讲

例1 设 F 是数域。F_∞ 是所有形如

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & \cdots \\ a_{21} & a_{22} & \cdots & a_{2n} & \cdots \\ \cdots & \cdots & \cdots & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} & \cdots \\ \cdots & \cdots & \cdots & & \end{pmatrix}, \quad a_{ij} \in F$$

的矩阵所构成的集合，其中，每个列只有有限个元不为 0。

（1）指出：$\{F_\infty; +, \cdot\}$ 是一个有单位元的环。其中，+ 和 · 分别为矩阵加法和乘法。

（2）设

$$a = \begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & 0 & \ddots \\ & & & \ddots \end{pmatrix} \quad b = \begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & 1 & 0 & \\ & & \ddots & \ddots \end{pmatrix}$$

（i）指出 b 是 a 的右逆元；

（ii）指出 a 没有左逆元。

解（1）首先指出矩阵的加法和乘法是F_∞的代数运算。为此只需证明：$\forall A, B \in F_\infty$ 必有 $A+B$，$AB \in F_\infty$ 即可。

因为 F_∞中的矩阵每个列只有有限个元不为0，不妨设 A 的第 j 列有 h_j 个元不为0，B 的第 j 列有 k_j 个元不为 0，于是 $A+B$的第 j 列至多有 h_j+k_j 个元不为0。因此，$A+B$ 的每个列只有有限个元不为0。即$A+B \in F_\infty$，所以矩阵的加法是F_∞的代数运算.

其次指出矩阵的乘法是 F_∞ 的代数运算。为此只需指出 AB的每个列只有有限个元不为0。

下面来看AB的第 j 列。设 B 的第 j 列中最后一个不为0的

元位于k_j行。因为A的每个列的不为0的元的个数有限，所以，A的前k_j个列中不为0的元的个数有限，设这些非0元分布在A的前h_j个行上。于是，A的前k_j个列的元从第h_{j+1}个以后都为0。即对$m>h_j$，A的第m行的前k_j个元都为0。由于在B的第j列中只有前k_j个元可能不为0，所以，在AB的第j列中，当$m>h_j$时，第m个元必为0。

综上所述，可知AB的第j列元素从第h_{j+1}个以后都为0。即AB的第j列上的元只有有限个不为0。所以$AB\in F_\infty$，即矩阵乘法是F_∞的代数运算。

容易验证$\{F_\infty;+,\cdot\}$是环。由乘法可知

$$e=\begin{pmatrix}1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \ddots\end{pmatrix}$$

是F_∞的单位元。

（2）（i）由乘法有：$ab=e$，所以b是a的右逆元。

(ii)因为，对于F_∞中的元

$$d=\begin{pmatrix}1 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & \ddots\end{pmatrix}$$

有$ad=0$，即a是F_∞的左零因子。因此，a不能有左逆元。这是因为，如果c是a的左逆元：$ca=e$，则有$(ca)d=ed=d$。

但$(ca)d=c(ad)=c0=0$，于是导出$d=0$的矛盾。

例 2　设$\{R;+,\cdot\}$是有1的环。对R规定新运算$\oplus$，$\odot$如下：

$a\oplus b=a+b-1$，$a\odot b=a+b-ab$，$\forall a,b\in R$ 证明，$\{R;\oplus,\odot\}$也是有1的环。

证明　因为$\{R;+,\cdot\}$是环，所以$a+b-1$和$a+b-ab$由a,b唯一确定而且是R中的元，即$\oplus$和$\odot$是R的代数运算。

其次，$\forall a,b,c\in R$

$$(a\oplus b)\oplus c=(a+b-1)\oplus c=(a+b-1)+c-1$$
$$=a+b+c-2\cdot 1$$
$$a\oplus(b\oplus c)=a\oplus(b+c-1)=a+(b+c-1)-1$$
$$=a+b+c-2\cdot 1$$

所以有 $(a\oplus b)\oplus c=a\oplus(b\oplus c)$，即$R$的加法$\oplus$满足结合律，而$\oplus$满足交换律是显然的。

因为，$\forall a\in R$，$a\oplus 1=a+1-1=a$，所以1是R的零元（对运算$\oplus$）。

下面说明R中每个元都有负元。$\forall a\in R$，如果有x使$a\oplus x=1$，则由$a\oplus x=a+x-1$ 有$a+x-1=1$，所以有，$x=2\cdot 1-a$。

上式说明，若x是a的负元，则$x=2\cdot 1-a$。

由$a\oplus(2\cdot 1-a)=1$，可知$\forall a\in R$，a在R中有负元存在。

综上所述，可知$\{R;\oplus\}$是加群。容易验证环的其它条件也成立，故$\{R;\oplus,\odot\}$是环。

$$\forall a\in R, a\odot 0=a+0-a0=a$$
$$0\odot a=0+a-0a=a$$

所以，0是$\{R;\oplus,\odot\}$的单位元。

例 3 设环R没有真零因子（既没有左零因子，又没有右零因子）。如果环R中的元$e\neq 0$满足条件：$e^2=e$，证明e是环R的单位元。

证明 $\forall x\in R, e(ex-x)=e^2x-ex=ex-ex=0$即$e(ex-x)=0$。

由题设，R没有真左零因子且$e\neq 0$，所以有

$$ex-x=0,\ 即ex=x$$

另一方面，

$$(x-xe)e=xe-xe^2=xe-xe=0$$

即$(x-xe)e=0$

再由题设，R没有真右零因子且$e\neq 0$，所以有：$x-xe=0$，即$xe=x$。

由上述可知 e 是环 R 的单位元。

例 4　设 R 为环，如果 R 中任意元都是幂等元：$\forall x\in R$，$x^2=x$，证明 R 是交换环。

证　要证 R 是交换环，只须证：$\forall a,b\in R$

$$ab=ba$$

即可。

$\forall a\in R$，由于 $(2a)^2=(a+a)^2=a^2+2a+a^2=4a$，$(2a^2)=2a$，所以，$4a=2a$。

由上式得到：$4a-2a=0$，即 $2a=0$。因此，由上式知：$\forall a\in R, a=-a$，即 R 中的元 a 的负元为 a。

另一方面，$\forall a,b\in R$

$$(a+b)^2=a^2+ab+ba+b^2=a+ab+ba+b$$

而　$(a+b)^2=a+b$，所以

$$a+b=a+ab+ba+b$$

于是得到

$$ab+ba=0$$

即　$ab=-ba$。但 $-ba=ba$（因为上面已证得：R 中每个元的负元是其本身），所以有：$ab=ba$。R 是交换环得证。

例 5　设 R 是环。$a\in R$，如果 $b\in R$ 使得

$$a+b-ab=0$$

则称 b 为 a 的右拟逆元。例如，0 的右拟逆元是 0。

证明　除环中的元除单位元 1 外，其余各元都有右拟逆元存在。

证明　设 R 为除环，$\forall x\in R$，若　$1+x-1\cdot x=0$，即 x 是 1 的右拟逆元，则有 $1=0$。而 R 是除环，与 $1\neq 0$ 相矛盾。上述说明，1 不能有右拟逆元。其次证明 $\forall a\in R$，当 $a\neq 1$ 时，a 存在右拟逆元。若　$a+x-ax=0$，则有

$$x(1-a)=-a \qquad (*)$$

因为 $a\neq 1$，所以 $1-a\neq 0$。由 R 是除环，所以 $1-a$ 在 R 中存在逆元：$(1-a)^{-1}$。于是由 $(*)$ 式得到

$$x=-a(1-a)^{-1}$$

而

$$a+\{-a(1-a)^{-1}\}-a\{-a(1-a)^{-1}\}$$
$$=a-a(1-a)^{-1}+a^2(1-a)^{-1}$$
$$=a-a(1-a)^{-1}(1-a)$$
$$=a-a=0$$

故 $-a(1-a)^{-1}$ 是 a 的右拟逆元。

例 6　设 $\{R;+,\cdot\}$ 是一个环，Z 是整数环。令 $\overline{R}=\{(m,a)\mid m\in Z,\ a\in R\}$，并且对 $\overline{R}$ 规定运算如下

$$(m,a)\oplus(n,b)=(m+n,a+b)$$
$$(m,a)\odot(n,b)=(mn,na+mb+ab)$$

证明

（1）$\{\overline{R};\oplus,\odot\}$ 是一个有 1 的环；

（2）R 与 $\overline{R}$ 的子环 R_1 同构，此处 $R_1=\{(0,a)\mid a\in R\}$。

证明　（1）首先，$\oplus$ 和 $\odot$ 是 $\overline{R}$ 的代数运算。

由于 $\overline{R}$ 的加法 $\oplus$ 是根据数的加法和环 R 的加法确定的，所以容易看出 $\overline{R}$ 的加法满足结合律也满足交换律。

而 $(m,a)\oplus(0,0)=(m,a)$，所以 $(0,0)$ 是 $\overline{R}$ 的零元；(m,a) 的负元是 $(-m,-a)$。

综上所述，可知 $\{\overline{R};\oplus\}$ 是加群。

其次验证 $\overline{R}$ 的乘法满足结合律。

因为

$$[(m,a)(n,b)](g,c)=(mn,na+mb+ab)(g,c)$$
$$=((mn)g,g(na+mb+ab)+(mn)c+(na+mb+ab)c)$$
$$=(mng,nga+mgb+gab+mnc+mbc+nac+abc)$$
$$(m,a)[(n,b)(g,c)]=(m,a)(ng,gb+nc+bc)$$
$$=(mng,nga+mgb+mnc+gab+mbc+nac+abc)$$

所以

$$[(m,a(n,b)](g,c)=(m,a)[(n,b)(g,c)]$$

即 $\overline{R}$ 的乘法满足结合律。

（在上面的推导中，为简便起见将乘法符号$\odot$略去）

类似地可以证明分配律成立。应用乘法可以看出$(1,0)$是$\overline{R}$的单位元。其中1是数，0是环R的零元。

（2）容易看出

$$\varphi: a \longmapsto (0,a),\ a\in R$$

是环R到R_1的同构映射。（R_1是$\overline{R}$的子环是显然的）

容易看出，环R与R_1在$\overline{R}$中的补集没有公共元，所以由本章§6定理3存在一个与$\overline{R}$同构的环$\overline{\overline{R}}$包含R。换句话说，任意没有单位元的环总可嵌入于一个有单位元的环中去。

例7　设环R除本身和$\{0\}$外，不再含其它左理想，证明：R是除环或幂零元环，即R中的每个元都是幂零元（$\forall x\in R$，存在正整数m使：$x^m=0$）。

证明　若$R=\{0\}$，命题显然成立。下面就$R\neq\{0\}$证明命题成立。$\forall a\in R$，令

$$Ra=\{ra \mid r\in R\}$$

显然，Ra是R的左理想。所以，由题设有

$$Ra=R,\ \text{或}Ra=\{0\}$$

上述说明，对于R中的任意元素a，或者$Ra=R$，或者$Ra=\{0\}$。

（1）若在R中有$a\neq 0$使：$Ra=\{0\}$时，则

$H=\{a \mid Ra=\{0\}\}$非空，而且$H\neq\{0\}$。

下面说明H是R的左理想。

$\forall a,b\in H \Longrightarrow Ra=\{0\}$，即　$r_1a=0$，$\forall r_1\in R$；$Rb=\{0\}$，即$r_2b=0$，$\forall r_2\in R$。而$\forall r\in R$，$r(a-b)=ra-rb=0\Longrightarrow R(a-b)=\{0\}$。所以$a-b\in H$，显然，$\forall a\in H$，$r\in R$。$ra\in H$。

上述说明：H是R的左理想。由于$H\neq\{0\}$，所以由题设有：$H=R$。由H的性质：$\forall a\in H$，$Ra=\{0\}$，即$\forall r\in R$，$ra=0$。所以，由$H=R$有：$\forall r_1r_2\in R\Longrightarrow r_1r_2=0$　特别地，$r^2=0$。即R是幂零元环。

（2）若对R中任意非零元a都有$Ra\neq\{0\}$，这时$\forall a(\neq$

$0)\in R$，恒有：$Ra=R$.

于是对于R中的任意元$a\neq 0$和b，方程

$$ya=b$$

在环R中有解。

因此，由本章§2习题9知R是除环。

显然，上例中的条件：R没有真左理想，换为R没有右理想时，命题的结论仍然成立。

例8 找出 $Z_6=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}$的所有理想。

解 首先，任一理想必包含零元：$\overline{0}$；

其次，如果Z_6的理想N包含单位元$\overline{1}$时，显然$N=Z_6$。如果Z_6的理想N包含$\overline{5}$时，则由$\overline{5}\cdot\overline{5}=\overline{1}$，所以$N=Z_6$。

另一方面，由于

$$\overline{2}+\overline{3}=\overline{5},\quad \overline{3}+\overline{4}=\overline{1}$$

所以，当Z_6的理想N同时包含$\overline{2}$和$\overline{3}$，或同时包含$\overline{3}$和$\overline{4}$时，则N也必为Z_6。

综合上述，可知Z_6的所有理想，除当然理想：Z_6和$\{\overline{0}\}$，只有下面两个

$$\{\overline{0},\ \overline{3}\};\ \{\overline{0},\ \overline{2},\ \overline{4}\}$$

例9 Z是整数环。令$R=\{(a,b)\,|\,a,b\in Z\}$，规定

$$(a,b)+(c,d)=(a+c,b+d);\quad (a,b)\cdot(c,d)=(ac,bd)$$

$$(a,b)=(c,d)\Longleftrightarrow a=c,b=d$$

则$\{R;+,\cdot\}$是一个环。

（1）证明，φ：$(a,b)\longmapsto a$，$\forall(a,b)\in R$是R到Z的满同态。

（2）求φ的核 $\mathrm{Ker}\varphi$。

证明（1）由于a由(a,b)唯一确定，所以φ是R到Z的映射。而且，$\forall a\in Z$有$(a,b)\in R$使：

$$(a,b)\longmapsto a$$

所以φ是满射。

下面说明φ是满同态。因为

$$\varphi((a,b)(c,d))=\varphi((ac,bd))=ac$$

$$\varphi((a,b))=a,\quad \varphi((c,d))=c$$

所以，$\varphi((a,b)(c,d))=\varphi((a,b))\varphi((c,d))$。因此，$R\sim Z$。

（2）$\forall(a,b)\in \mathrm{Ker}\varphi$，因为

$$\varphi((a,b))=a=0,\quad \varphi((0,b))=0$$

所以，$\mathrm{Ker}\varphi=\{(0,b)\mid b\in Z\}$。

例10　设 $R=\{a+b\sqrt{-2}\mid a,b\in Z\}$，则 $\{R;+,\cdot\}$是一个环，其中“+”和“·”分别为数的加法和乘法。

对R中的任意元 $\alpha=a+b\sqrt{-2}$，规定

$$\delta(\alpha)=a^2+2b^2$$

证明，R是欧氏环。

证明　R是交换环，$1=1+0\cdot\sqrt{-2}$是R的单位元。由于R是数环，所以R没有真零因子。因此R是整环。

由题设，对于每一 $\alpha=a+b\sqrt{-2}\neq 0$，显然 $\delta(\alpha)=a^2+2b^2>0$，即$\delta(\alpha)$为正整数（因为，$a,b\in Z$）。

下面证明，对于R中的任意元α和$\beta\neq 0$，在R中存在q和r，使得

$$\alpha=\beta q+r$$

而且，$r=0$，或者$\delta(r)<\delta(\beta)$。设$\alpha=a+b\sqrt{-2}$，　$\beta=c+d\sqrt{-2}\neq 0$，则

$$\beta^{-1}\alpha=\frac{a+b\sqrt{-2}}{c+d\sqrt{-2}}=\frac{(a+b\sqrt{-2})(c-d\sqrt{-2})}{c^2+d^2}$$

$$=\frac{(ac+2bd)+(bc-ad)\sqrt{-2}}{c^2+d^2}=k+l\sqrt{-2}\qquad(1)$$

其中，$k=\dfrac{ac+2bd}{c^2+d^2}$，　$l=\dfrac{bc-ad}{c^2+d^2}$ 是有理数。令k'和l'是满足条件：

$$|k-k'|\leqslant\frac{1}{2},\quad |l-l'|\leqslant\frac{1}{2}$$

的两个整数。

根据有理数的性质，容易看出对任意有理数 $k=\frac{t}{s}$ 来说，总有：$k=\frac{t}{s}=k'+\frac{t'}{s}$，此处 k' 是整数，$t'<s$ 即任意有理数总可表为一个整数与真分数之和。如果 $\frac{t'}{s}\leqslant\frac{1}{2}$，则 $|k-k'|\leqslant\frac{1}{2}$。如果 $\frac{t'}{s}>\frac{1}{2}$，则 $1-\frac{t'}{s}<\frac{1}{2}$。所以

$$|k-(k'+1)|<\frac{1}{2}$$

下面指出，在 R 中存在 q 和 r 使得 $\alpha=\beta q+r$，或者 $r=0$，或者 $\delta(r)<\delta(\beta)$。令(2) $q=k'+l'\sqrt{-2}$，$r=\alpha-\beta q$。显然 q，$r\in R$。

最后证明：当 $r\neq0$ 时，$\delta(r)<\delta(\beta)$。我们从题设中知道，$\delta(\alpha)=a^2+2b^2$，事实上，就是复数 $\alpha=a+b\sqrt{-2}$ 的模的平方。因此，对任意复数 $c+d\sqrt{-2}$，$\delta(\alpha)$ 都有意义。其中，c 和 d 是任意实数。并且，只要 $c+d\sqrt{-2}\neq0$，$\delta(\alpha)=c^2+2d^2$ 是正实数。根据模的性质，对于任意 α,β，都有 $\delta(\alpha\beta)=\delta(\alpha)\delta(\beta)$，而

$$\begin{aligned}\delta(r)&=\delta(\alpha-\beta q)=\delta(\beta(\beta^{-1}\alpha-q))=\delta(\beta)\delta(\beta^{-1}\alpha-q)\\&=\delta(\beta)\delta((k-k')+(l-l')\sqrt{-2})\text{（由(1)和(2)）}\\&=\delta(\beta)((k-k')^2+2(l-l')^2)\\&\leqslant\delta(\beta)\left(\left(\frac{1}{2}\right)^2+2\cdot\left(\frac{1}{2}\right)^2\right)=\delta(\beta)\left(\frac{1}{4}+\frac{1}{2}\right)\\&=\frac{3}{4}\delta(\beta)<\delta(\beta)\end{aligned}$$

综合上述，可知 R 是欧氏环。

在本章§11例4中，我们曾指出

$$I=\{a+b\sqrt{-3}\mid a,b\in Z\}$$

不是唯一分解环。而上面的例10指出 $R=\{a+b\sqrt{-2}\mid a,b\in Z\}$ 是欧氏环，从而是唯一分解环。由于这两个环从外形上很相象，也许会想到，如果对§11例4的整环 I 规定：$\delta(\alpha)=a^2+3b^2$，$\alpha=a+b\sqrt{-3}$。那么，能否类似于本例的证明，证出 I 也是欧氏环呢？事实上，§11例4已明确 I 不是唯一分解环，当然决不会证出 I 是欧氏环。

另一方面，按本例的办法，当

$$\alpha=\beta q+r$$

时，证不出 $\delta(r)<\delta(\beta)$。

这是因为，对 I 来说，按例10的作法

$$\begin{aligned}\delta(r)&=\delta(\alpha-\beta q)=\delta(\beta(\beta^{-1}\alpha-q))=\delta(\beta)\delta(\beta^{-1}\alpha-q)\\&=\delta(\beta)\ \delta((k-k')+(l-l')\sqrt{-3})\\&=\delta(\beta)((k-k')^2+3(l-l')^2)\\&\leqslant\delta(\beta)\left(\left(\frac{1}{2}\right)^2+3\cdot\left(\frac{1}{2}\right)^2\right)=\delta(\beta)\left(\frac{1}{4}+\frac{3}{4}\right)=\delta(\beta)\end{aligned}$$

即 $\delta(r)\leqslant\delta(\beta)$，不能保证总有：$\delta(r)<\delta(\beta)$。

所以，不能简单地只就一个代数体系的外形，而妄下结论。

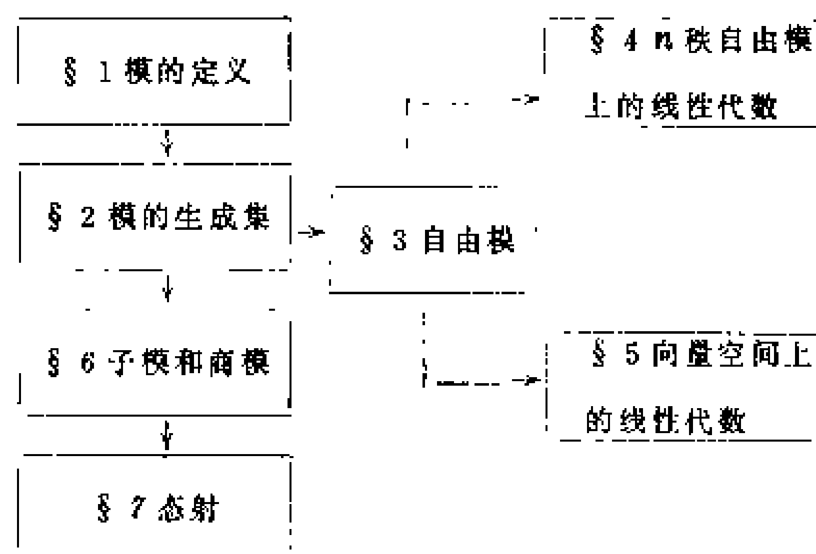
第四章 模学习指导

一 内容概要

模是由环和加群在倍乘运算下所组成的代数体系，是“高等代数”中，数域上线性空间概念的发展和推广。在数域上的线性空间中，将数域的条件推广到一般的环上。具体说来，是放弃了数域所具有的：（1）乘法的可换性，（2）非零元素的可除性，（3）乘法单位元的存在性，（4）元素个数的无限性等性质，来做成比线性空间更加广泛的代数体系—模。

因此，学习本章时，要对照线性代数中有关章节进行。既要考查模在数域上线性空间中所继承下来的性质，又要比较数域推广成环后所产生的新的性质。

本章各节间的联系如下图：



另一方面，模也是特殊的加群，是藉助于环 R，赋予加群

M中元素以线性关系的群．有的书就将模叫作带算子群．同时，任一加群也都可以看作特殊的模：Z—模．因此对模的研究也是对加群研究的深入．又因为任一个环都是一个特定的模—环模，环的任一理想也都可视为子模．所以对模的研究也是对环的研究的继续；环R的理想与模的子集间的联系已成为"代数几何"的建立基础和研究的基本手段．

模的理论发展到现在，已成为数学中一个基础学科．

二 内容分析

§1 模的定义

（一）内容提要

本节给出了模的定义和运算，并进一步对模的性质作讨论．明确了我们研究的重点应该放在有$1\neq 0$环上的左单式模上．

1 模的定义

参照数域上线性空间的定义，将数域这样一个特殊的环，推广成一般的环．由于一般环不一定有1，故去掉了线性空间中条件

（4）$1x=x$，$\forall x\in V$

这样便得到了包蕴线性空间在内的更加广泛的代数体系—模．

2 模的运算基本性质

由于环上的模保留了数域上线性空间中倍乘关于加法的分配律，故在模中同数域上线性空间一样，可直接推出两条运算基本性质

（1）$a\theta=ox=\theta$

（2）$(-a)x=a(-x)=-(ax)$

$\forall x\in M$，$a\in R$都成立．

3　重点研究的模

（1）对环上一般模的研究，可转化为对环上单式模的研究。

称满足条件 $RM=M$ 的模为 R 上的单式模。在有 1 环 R 上，单式模就是满足条件

$$1x=x\quad \forall x\in M$$

的模。

对于有 $1\neq 0$ 的环 R，其上的模 M 可分解为

$$M=M_0\oplus M_1$$

M_0 是零模，结构是清楚的，M_1 是单式模。于是对 M 的研究转化为对单式模 M_1 的研究。

（2）对右模的研究，可以通过对左模的研究得到解决。

通过对左模和右模的差别和联系的讨论，明确了左模上的理论可平行地移到右模上，于是明确了重点研究环 R 上的左单式模就可以了。

（二）补充说明

1　在数域上线性空间中有运算性质

$$ax=\theta\Longrightarrow a=0\text{或}x=\theta$$

在环 R 上的模 M 中，就不一定成立了。如对于 $M_n(\boldsymbol{Z})$—模 $\boldsymbol{Z}^{(n)}$，取

$$x=(1,0,\cdots,0)\in\boldsymbol{Z}^{(n)}$$

$x\neq\theta$。再取

$$\boldsymbol{A}=\begin{pmatrix}0&\cdots&0&1\\0&\cdots&0&0\\\cdots&\cdots&\cdots&\cdots\\0&\cdots&0&0\end{pmatrix}\in M_n(\boldsymbol{Z})$$

也有 $A\neq 0$，但却有

$$A\cdot x=xA'=\theta\quad(\S\,1\ \text{例}10)$$

2　对左模和右模的说明

左模和右模的区别，在于标量之积倍乘模元素分解成标量因子逐次倍乘时，其顺序是由右逐次向左进行，还是逐次由左向右进行，若是由右向左进行则为左模，若是由左向右进行则为右模。

在可换环R中，标量之积与标量顺序无关，因此R上的左模也是R上的右模。标量a与模元素倍乘之积记作ax或xa都可以，对数域上线性空间，我们不去强调是左的，还是右的就是这个道理。例 6 和例 8 就是说的这种情形。

在非交换环R中，标量之积与标量顺序有关。因此在左模中，标量与模元素之积即使将标量记在模元的右侧，也不能成为右模。例 7 和例 9 就是说的这种情形。

3　对几个例题的说明

例11指出任何一个加群都可以视为Z—模，例12是说任一环的理想都可以作成该环上的模，例13指出对环的理想所带来的商环，其加群也可以看作环上的模。

这些例子会使你感到，模是一个容量很宽、联系很广的数学概念，也可使你通过这些例子，初步地掌握由一已知环去构造模的简单方法。

§ 2　模的生成集

（一）内容提要

本节主要研究模的构造。作为加群的模M，籍助于环R，赋予模元素一个线性关系，于是可用部分模元素通过环R线性组合成一批新的元素。由此导入R—模M的生成集的概念。它籍助于R所赋予的线性关系，建立了模的部分元素——生成集和整体的关系，给出了模元素的表示，显示出模在环上的结构，从中也可以看出在环上构造模的基本方法。

本节所论述的问题

1　模的生成集的定义及生成集的存在性；

2　关于模的生成集所含模元素数量的讨论，给出了有限生成模和无限生成模的概念。

3　提出了最小生成集的概念，其存在性可通过习题5去解决。

4　讨论了最小生成集和数域上线性空间基底的不同，为下节自由模的引入作一先导。

（二）补充说明

1　模的生成集的定义是针对环 R 上单式模而言的。一般环上非单式模是不存在这样定义的生成集的。如

设 $M=\boldsymbol{Z}_2=\{\overline{0},\overline{1}\}$，是以2为模的剩余类加群，$R=\{a\in\boldsymbol{Z}\mid a=2n,\forall n\in\boldsymbol{Z}\}$ 是偶数环。关于倍乘运算：

$$a\,\overline{x}=\overline{ax}\quad\forall a\in R,\ x\in M$$

M 构成 R 上的零模，是非单式模。对于模元素 $\overline{1}\neq\overline{0}$，不可能通过 $\boldsymbol{Z}_2$ 中的元素组线性表示出来，所以 R—模 $\boldsymbol{Z}_2$ 不存在所定义的那种生成集。

关于一般模，“生成”的形式将比这稍复杂些。

§3　自　由　模

（一）内容提要

对于有 $1\neq0$ 的环 R 上的有限生成单式模 M 来说，研究起来仍很复杂。其困难在于：（1）最小生成集所含模元素个数未必唯一；（2）模元素在最小生成集上的线性表示式也不一定是唯一的。为克服上述两点困难，对有限生成单式模再加以强化，提出一类特殊的模——自由模。

本节所论述的问题：

1　模元素在 R 上的线性关系

这一部分是给自由模概念的提出作准备的，与数域上线性空间一样，导入了线性组合，线性表出，线性相关和线性无关

等基本概念

2　自由模的定义

对于有限生成的R—模M来说，线性无关的子集$\{x_i\}_{i=1}^n$线性表出任一模元素时，表法是唯一的。这就启示我们，要想使R—模M的生成集表出任一模元素时，具有表法唯一的特点。只要对该生成集加上线性无关的限制条件就可以了。于是引进了具有线性无关的有限生成集的模—自由模。

3　有$1\neq0$交换环上自由模的秩

对自由模来说，各自由基所含模元素个数相等是导入秩的概念的基础，这一定理是在有$1\neq0$的交换环上证明的，由此给出了秩的定义。

（二）补充说明

1　在R—模M中，关于线性关系的几个概念，是数域上线性空间中有关概念的直接引入，但由数域推广成环，使：（1）非零元不一定可逆；（2）可能存在零因子；（3）可能存在真理想，…。于是使数域上线性空间中，线性关系的一些性质没能完整的继承下来。对此，本书就环模N_6，举了两个例子，告诉读者不能轻率的将数域上线性空间中的一些熟知的结论搬到环上的模中。

2　例1—例4给出了如何就自由模的定义去判断一个模是否是自由模。其关键就是检验环上的模是否存在线性无关的有限生成集。

3　对习题3要予以注意，从中可以看到自由模中，作为自由基的模元素，条件是比较严格的。在数域上线性空间中，只要是非零向量，就可以作为一个基底向量而含在某个基底中；而在环R上的自由模M中，非零模元素可能是非自由元，因而非零模元素不一定都能作为自由基的元素而含在某自由基中。以后还可看到，即使是自由元，也不一定能作为自由基中元素含在某自由基中。

§4　n秩自由模上的线性代数

（一）内容提要

本节的主要工作是将数域上线性空间中的一些结果推广到n秩自由模上。

数域是一个交换除环，n秩自由模所在的环是有$1\neq0$的交换环。因此在推广过程中，要注意环的不可除性所带来的特点。

本节所论述的问题

1　模元素的坐标表示

（1）对于n秩自由模R—模M，取定自由基$U=\{u_i\}_{i=1}^n$后，任一模元素x，都被x在U上的坐标$[x]_U$所唯一确定。

（2）R—模M中的运算可以通过坐标的运算来实现。

（3）自由基$U=\{u_i\}_{i=1}^n$通过阵A演化为自由基$V=\{v_i\}_{i=1}^n$时，坐标变化规律为

$$[x]_U=[x]_V A$$

2　R—自同态及其矩阵表示

（1）R—自同态的定义。

（2）R—自同态的矩阵表示。设φ是n秩自由模M的R—自同态，$U=\{u_i\}_{i=1}^n$是R—自由基。则R—自同态φ在U上矩阵表示式为：

$$[\varphi(x)]_U=[x]_U\mathrm{Mat}_U(\varphi)$$

（3）当自由基U通过可逆阵C演化为自由基V时，φ的阵的变化规律为

$$\mathrm{Mat}_V(\varphi)=C[\mathrm{Mat}_U(\varphi)]C^{-1}$$

3　R—自同态所构成的代数

（1）在$\mathrm{End}_R(M)$中，引进了加法运算，乘法运算和R中标量对$\mathrm{End}_R(M)$中R—自同态的倍乘运算。它们满足下列算律

$\mathrm{End}_R(M)$构成环R上的模，且

$$\varphi(\psi+\rho)=\varphi\psi+\varphi\rho$$

$$(\psi+\rho)\varphi=\psi\varphi+\rho\varphi$$

$\forall\quad \varphi,\ \psi、\rho\in \mathrm{End}_R(M)$

$$(a\varphi)\psi=\varphi(a\psi)=a(\varphi\psi)$$

$\forall\quad a\in R,\ \varphi,\psi\in \mathrm{End}_R(M)$.

符合环R上代数的定义，所以$\mathrm{End}_R(M)$构成了环R上的代数。

（2） R上n阶阵集合$M_n(R)$，也构成环R上的代数。

（3） 在映射

$$\mathrm{mat}_V:\ \mathrm{End}_R(M)\longrightarrow M_n(R)$$

$$\varphi\longrightarrow \mathrm{Mat}_V(\varphi)$$

下，$\mathrm{End}_R(M)$与$M_n(R)$是反同构代数。

（二） 补充说明

1 本节给出了R—n秩自由模M的模元素坐标表示和M上的R—自同态的矩阵表示。将M中的模元素和M上的R—自同态用R中的一些标量具体表出。“标量化”了的模元素和R—自同态不仅表示具体，而且在运算上也转化为R中标量的运算（即模元素坐标行的运算和R—自同态的阵的运算，都是通过R中标量的运算来实现的）.运算也具体化了。表示具体，运算具体，这就是模元素和R—自同态“标量化”的意义。“标量化”的缺欠是使模元素和R—自同态失去了原有的几何形象，对藉助于几何形象去探讨问题很不利。这就是不能用坐标和阵完全取代模元素和R—自同态的原因。

2 本节中，并未涉及环R的可除性问题。这容易造成错觉，数域上线性空间的结论都可推广到自由模上。其实并不这样，上节就看到了由环的不可除性所引起的模元素线性关系性质的改变；再看数域上阵的初等变换。为了将阵中某元素化为1常用到某元素的逆元。这在非除环中，就不能进行了。由此可知，一般交换环R上，n秩自由模M的R—自同态φ的标准型问题（也就是R上n阶阵的标准型），将是一个很难的问

题，当前也是很多数学工作者感兴趣的问题之一。

3　R—自同态代数 $\mathrm{End}_R(M)$ 与 R—矩阵代数 $M_n(R)$ 在映射

$$\mathrm{Mat}_V: \mathrm{End}_R(M) \longrightarrow M_n(R)$$
$$\varphi \longrightarrow \mathrm{Mat}_V(\varphi)$$

下是反同构。由此可知，对 R—自同态代数 $\mathrm{End}_R(M)$ 的研究和对 R—矩阵代数 $M_n(R)$ 的研究可以互相转化。

对 R—矩阵代数 $M_n(R)$，研究起来对象明确，运算具体；对 R—自同态代数研究起来形象鲜明（如位似变换，反射变换，平延变换，…），可藉助形象来帮助你思考论证。这两种方法，虽然在不同学派各有所侧重，但对一些问题往往是交替使用的。

§5　向量空间上的线性代数

（一）内容提要

除环 K 上向量空间 V，是又一类比较近于数域上线性空间的模，是将数域推广成不一定可交换的除环上所得的模。所以在学习时，要注意不可换性所引起的后果。

本节内容是这样编排的

1　除环 K 上 n 维向量空间。

（1）先证明了除环 K 上有限生成模存在线性无关生成集，由此引进 K—基的概念；

（2）其次证明了 K—向量空间 V 的两个 K—基含有相同个数的向量，由此引进了 K—向量空间维数的概念；

（3）K—基的演化规律：令 $X=\{x_i\}_{i=1}^n$ 和 $Y=\{y_i\}_{i=1}^n$ 是 K—向量空间的两个 K—基

$[y_i]_X=(c_{i1}, c_{i2},\cdots,c_{in})$　$i=1,2,\cdots,n$，则阵 $C=(c_{ij})$ 是可逆阵，称为由 X 到 Y 的演化阵。

2　向量坐标表示

（1）向量 x 在 V 的 K—基 X 上，由其坐标 $[x]_X$ 所唯一确定；

（2）向量运算可通过坐标运算来实现

$[x+y]_X=[x]_X+[y]_X$

$[kx]_X=k[x]_X$

（3）K—基 X 通过阵 C 演化为 K—基 Y，向量 x 的坐标变化规则为

$[x]_X=[x]_YC$

3　线性变换及其矩阵表示

（1）K—向量空间 V 上的线性变换定义；

（2）线性变换在 K—基上的矩阵表示式

$[\varphi(x)]_X=[x]_X\mathrm{Mat}_X(\varphi)$

（3）K—基的演化对线性变换阵的影响，若 K—基 X 到 K—基 Y 的演化阵为 C。φ 是 V 上的线性变换，且 $\mathrm{Mat}_X(\varphi)=A$，$\mathrm{Mat}_Y(\varphi)=B$ 则有 $B=CAC^{-1}$。

4　V 上线性变换代数

（1）线性变换的运算

（i）关于加法 $\mathrm{End}_R(V)$ 成群；

（ii）K 的中心子域 Δ 对 $\mathrm{End}_R(V)$ 的倍乘，使 $\mathrm{End}_R(V)$ 构成 Δ 上的模；

（iii）关于乘法 $\mathrm{End}_R(V)$ 成环。

总之，$\mathrm{End}_R(V)$ 构成了 K 里的线性变换代数，

5　$M_n(K)$ 也构成 K 里的代数，称之谓矩阵代数。

6　$\mathrm{End}_R(V)$ 与 $M_n(K)$ 在映射 Mat_X 下是反同构的代数，于是可将 $Mn(K)$ 看作 $\mathrm{End}_K(V)$ 的具体表示。

（二）补充说明

本节关于向量的坐标表示和线性变换的矩阵表示，可参看前节的有关说明，这里不去重述。此外

1　在交换环 R 上，n 秩自由模 M 的 R—自同态变换加群 $\{\mathrm{End}_R(M),+\}$ 可以作成 R 上的自由模，而在除环 K 上，n 维向

量空间V的线性变换加法群$\{End_K(V), +\}$为什么不能作成K上的模，而只能作成K的中心子域Δ上的模呢？

这是因为：K是不可换的，则必存在a，$b \in K$使$ab \neq ba$，如果$End_K(V)$作成K上的模，则有$\varphi \in End_K(V)$，$\varphi \neq 0$，使$a\varphi \in End_K(V)$，此时，$\forall x \in V$都有

$$(a\varphi)(bx) = b(a\varphi(x)) = (ba)\varphi(x)$$

但是

$$(a\varphi)(bx) = a(\varphi(bx)) = a(b\varphi(x)) = (ab)\varphi(x)$$

于是有

$$(ba)\varphi(x) = (ab)\varphi(x)$$

由$ba \neq ab$。知$\varphi(x) = \theta$，与$\varphi \neq 0$矛盾。故$End_K(V)$不能作成K上的模。

2　在交换环R上的n秩自由模M中，R—自同态加群$Eud_R(V)$作成R上的n^2秩自由模；而在除环K上，n维向量空间V中，线性变换加群$End_K(V)$所作成的，K的中心Δ上的模，就不一定再是n^2维的了。如令

$$K = \left\{\begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} \in M_2(C) \mid \alpha, \beta \in C\right\}, C\text{是复数域。}$$

则K是一个除环。中心子域

$$\Delta = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in R \right\}, R\text{是实数域。}$$

考查K的加法群在K上的向量空间，维数是1。而$End_K(K)$在Δ上的维数，就是4维的了。

§6　子模和商模

（一）内容提要

为了考察R—模M的结构，提出了子模的概念。有了M的子模N就给M的元素一个分类。在所构成的商集中，引进合理的运算，使之构成商模，用以建造R—模M的同态象。同态象

是R一模M的一个“缩影”，是考察R一模M的“门径”。本节所论述的问题：

1　子模：（1）子模的定义；（2）子模的判定条件；（3）子模的构造方法；（4）子模的合成。

2　商模：这里给出了根据子模N，去建造商模的过程和方法。

（1）商模的元素

设N是R一模M的子模，则关于模N的加法运算，N构成加群M的正规子群。N在M里的陪集：$x+N$，$x\in M$作成商模的元素；由陪集构成的商集：$M/N=\{x+N\mid\forall x\in M\}$作成商模的模元素集。

（2）商模的运算：加和倍乘

（i）$\forall\ x+N,\ y+N\in M/N$，规定

$$(x+N)+(y+N)=(x+y)+N$$

则$\{M/N,+\}$是一个加群。

(ii)　$\forall\ x+N\in M/N,\ r\in R$，规定

$$r(x+N)=rx+N$$

则加群M/N在倍乘运算下构成环R上的模。

（二）补充说明

1　与数域上线性空间的子空间比较，环上模的子模的内容和形式要丰富得多。数域上线性空间中很多几何观念被冲破了，很多代数性质也被破坏了，就拿n秩自由模来说，如　Z一模$Z^{(3)}$其中

$$L_1=\{(x,0,0)\mid x\in Z\}$$

是$Z^{(3)}$的1秩自由子模。

$$K_1=\{(2y,0,0)\mid y\in Z\}$$

也是$Z^{(3)}$的1秩自由子模。但$L_1\supset K_1$；而在实数域R上的线性空间$R^{(3)}$中，任一个一维子空间（过原点的直线）不能真包含1维子空间（直线）。又

$$L_2=\{(2x,2x,0)\mid x\in Z\}$$

$$K_2=\{(3y,3y,0)\mid y\in Z\}$$

是 $Z^{(3)}$ 的二个1秩自由子模。但是

$$L_2\cap K_2=\{(6z,6z,0)\mid z\in Z\}$$

其交点有无穷多。而在R—线性空间$R^{(3)}$中二个不同的一维子空间的交点只能有一个（0,0,0）（两条不同直线交点最多是一个）。

由此看来环上的几何学要比数域上的几何学丰富得多了。

2　关于子模的合成

子模的合成是通过已知子模去构造新子模的手段，更为重要的在于给出子模间的连系方法和关联形式。一个模分解成子模的直和，是表示模的结构的根本手法。如除环K上线性空间$K^{(3)}$可以表成

$$K^{(3)}=Ke_1\oplus Ke_2\oplus Ke_3$$

$e_1=(1,0,0)$，$e_2=(0,1,0)$，$e_3=(0,0,1)$，这样，$K^{(3)}$在K上的结构就清晰了。

§7　态　　射

（一）内容提要

模是加群M和环R在倍乘运算下所成的代数体系。态射是用来对两个模进行比较和建立联系的一种映射。因此，这个映射既要反映出两个加群间保持运算的映射关系。又要反映出两个环之间的联系。

本节采取由特殊到一般的过程，渐次建立起态射概念。

1　R—自同态

R—模M的R—自同态φ，是M自身的一种变换。对加群M保持同态。即

（1）$\varphi(x+y)=\varphi(x)+\varphi(y),\forall x,y\in M$

对φ下的标量因子r可以完整的析出，即

（2）$\varphi(rx)=r\varphi(x)$，$\forall x\in M,r\in R$

2　R—同态

R—模 M_1 到 R—模 M_2 的 R—同态 φ，是 M_1 到 M_2 的一种映射，对模的加法来说保持运算

（1）$\varphi(x+y)=\varphi(x)+\varphi(y)$，$\forall\ x,y\in M_1$

对 φ 下的标量因子 r 可以完整的析出，

（2）$\varphi(rx)=r\varphi(x)$。$\forall r\in R$，$x\in M_1$

R—同态映射是模论中基本的常用的映射，R—同态基本定理是模论中基础定理之一。

R—同构的模，是具有相同代数性质的模，是在代数意义下相等的模。

对于 n 秩自由模来说，R—同构的充要条件是秩数相等，因而 R—模 $R^{(n)}$ 成了交换环 R 上的 n 秩自由模的代表。

对于 n 维向量空间来说，K—同构的充要条件是维数相等，因而 K—向量空间 $K^{(n)}$ 成了除环 K 上的 n 维向量空间的代表。

3　关于 σ 的 R—半同态

对于 R—模 M_1 到 R—模 M_2 的映射 φ。关于模的加法保持运算

（1）$\varphi(x+y)=\varphi(x)+\varphi(y)$　$\forall x,y\in M_1$

对 φ 下的标量因子 r 可以析出，但是不能完全不变的析出，必须在析出后经 R 的自同构 σ 加以变化，即

（2）$\varphi(rx)=\sigma(r)\varphi(x)$　$\forall x\in M$，$r\in R$

4　态射

"σ—态射 φ" 是 R_1—模 M_1 到 R_2—模 M_2 的映射。在 φ 下，M_1 和 M_2 保持加法运算，即

（1）$\varphi(x+y)=\varphi(x)+\varphi(y)$　$\forall\ x,y\in M_1$

对 φ 下 R_1 的标量因子 r，析到 φ 的外面需按环 R_1 到环 R_2 的同态映射 σ，变成 R_2 里的标量才可以，即

（2）$\varphi(rx)=\sigma(r)\varphi(x)$　$\forall x\in M_1, r\in R_1$

（二）补充说明

1　态射是一个意义广泛的映射

对于环 R_1 上的模 M_1 和环 R_2 上的模 M_2

$$\sigma: R_1 \to R_2$$

是环同态；

$$\varphi: M_1 \to M_2$$

是群同态。如果 $\forall\ x \in M_1,\ r \in R_1$ 有

$$(2)\qquad \varphi(rx) = \sigma(r)\varphi(x)$$

则称 φ 为 σ—态射 φ。

（i）当 $R_1 = R_2 = R$，σ 是同构时，φ 是关于 σ 的 R—半同态；

(ii) 当 $R_1 = R_2 = R$，σ 是恒等自同构时，φ 是 R—同态；

(iii) 当 $R_1 = R_2 = R$，σ 是恒等自同构，$M_1 = M_2 = M$ 时，φ 是 R—自同态。

2　态射的矩阵表示

在§4和§5中对 n 秩自由模和 n 维向量空间的 R—自同态和线性变换，研究了矩阵表示。同样对 n 秩自由模或 n 维向量空间来说，态射也能用矩阵表示出来。下面仅就 n 秩自由模上的关于 σ 的 R—半自同态作一下。

设 R—M 是 n 秩自由模，$U = \{u_i\}_{i=1}^n$ 是 R—自由基。φ 是关于 σ 的 R—半自同态。如果

$$[\varphi[u_i]]_U = (a_{i1}, a_{i2}, \cdots, a_{in}) \quad (i = 1, 2, \cdots, n)$$

则 $A = (a_{ij})$ 称为 σ—半同态 φ 在 R—自由基 U 上的阵。此时，对 $x = \sum_{i=1}^n b_i u_i \in M$，有

$$\varphi(x) = \varphi\left(\sum_{i=1}^n b_i u_i\right) = \sum_{i=1}^n \sigma(b_i)\varphi(u_i)$$

于是得 σ—半同态 φ 的矩阵表示式

$$[\varphi(x)]_U = [x]_U^\sigma A$$

其中 $[x]_U = (b_1, b_2, \cdots, b_n)$，$[x]_U^\sigma = (\sigma(b_1), \sigma(b_2), \cdots, \sigma(b_n))$

由此知，R—模 M 的半同态，被阵 A 和 R 的自同构 σ 所

唯一确定。令Aut(R)表示环R的自同构集合，则

$$\varphi \longrightarrow (\sigma, A)$$

是“R—n秩自由模M上的R—半同态集合”，到 $\mathrm{Aut}(R) \times M_n(R)$的双射。给出合理的运算，则 $\mathrm{Aut}(R) \times M_n(R)$又将构成$R$上新的代数体系。这里就不作新的介绍了。

3　对例6的说明

我们通过

$$\sigma: R \to \overline{R} = R/B$$

$$r \to \overline{r} = r + B, \quad \forall \ r \in R$$

和

$$\varphi: \ M \to \overline{R}^{(n)}$$

$$x = \sum_{i=1}^{n} a_i u_i \to (\overline{a_1}, \overline{a_2}, \cdots, \overline{a_n}), \quad \forall \ x \in M$$

建立了R—模M到$\overline{R}$—模$\overline{R}^{(n)}$的φ下的σ—态射。建立了通过$\overline{R}$—模$\overline{R}^n$去窥测R—模M的渠道。这是研究n秩自由模的一个很基本的途径。尤其是当取B为R的极大理想时。$\overline{R} = R/B$是域，$\overline{R}^{(n)}$是$\overline{R}$上的向量空间。对于域上的n维向量空间，我们是很清楚的。这样便可以通过$\overline{R}$—向量空间$\overline{R}^{(n)}$去考查R—模M了。习题7就是这方面的一个实例。

三　例题选讲

例1　令R是有$1 \neq 0$的交换环，R—模M是单式模，$L(x)$和$L(y)$分别由模元素x和y生成的循环模

$$O(x) = \{a \in R \mid ax = \theta\}$$

$$O(y) = \{b \in R \mid by = \theta\}$$

是R中的x和y的阶理想。

（1）如果$L(x) = L(y)$，则$O(x) = O(y)$；

（2） $L(x)=L(y)$ 必要而且只要 $y=rx, x=ly, r, l\in R$；

（3） $L(x)=L(y)$ 必要而且只要 $y=rx, r\in R$ 且 $\bar{r}=r+O(x)$ 在商环 $R/O(x)$ 中是可逆元；

（4） 举例说明：如果 $O(x)=O(y)$，则 $L(x)=L(y)$ 不一定成立。

解 （1） 由 $L(x)=L(y)$ 知

$$\{ax \mid a\in R\}=\{by \mid b\in R\}$$

又 R 是有 1 的环，M 是单式模，知

$$x=1x\in L(x)=\{by \mid b\in R\}$$

故存在 $r\in R$ 使 $x=ry$，同理可知存在 $l\in R$ 使 $y=lx$。此时如果 $a\in O(x)$，则 $ax=\theta$。于是有 $ay=a(lx)=(al)x=(la)x=l(ax)=\theta$。故 $a\in O(y)$。即 $O(x)\subseteq O(y)$。同样亦可证得：$O(y)\subseteq O(x)$。从而得 $O(x)=O(y)$。

（2） 必要性见（1），现证充分性。由 $x=ry$ 知 $ax=a(ry)=(ar)y\in L(y)$，$\forall a\in R$ 都成立。故 $L(x)\subseteq L(y)$，同理可得，$L(y)\subseteq L(x)$，故得 $L(x)=L(y)$。

（3） 必要性。由 $L(x)=L(y)$ 可推得：存在 $r, l\in R$ 使 $x=ry, y=lx$，于是有 $x=ry=r(lx)=(rl)x$ 又因为 R 是有 1 的环，M 是单式模。所以又有 $x=1x$。从而得

$$(1-lr)x=\theta$$

于是知 $1-lr\in O(x)$，$\bar{r}\ \bar{l}=\bar{1}$，$\bar{r}$ 是 $R/O(x)$ 中的可逆元。

充分性。由 $y=rx$ 知 $L(y)\subseteq L(x)$。又在 $R/O(x)$ 中存在 $\bar{l}=l+O(x)$，使 $\bar{l}\ \bar{r}=\bar{1}$。于是知 $lr-1\in O(x)$，$(lr-1)x=\theta$ 故

$$x=(lr)x=l(rx)=ly$$

得 $L(x)=L(y)$。

（4） 考查 Z_6—模 $Z_6^{(2)}$

取 $x=(\bar{2}, \bar{0})$ $y=(\bar{0}, \bar{2})$，于是

$$O(x)=\{\overline{0},\ \overline{3}\}=O(y)$$

但是

$$L(x)=\{(\overline{0},\ \overline{0}),\ (\overline{2},\ \overline{0}),\ (\overline{4},\ \overline{0})\}$$

$$L(y)=\{(\overline{0},\ \overline{0}),\ (\overline{0},\ \overline{2}),\ (\overline{0},\ \overline{4})\}$$

所以 $L(x)\neq L(y)$。

再举一例　令$M=\{0,a,b,c\}$是4元群，运算表为

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

则交换群M可以看作$\boldsymbol{Z}$—模，于是有

$$O(a)=O(b)=O(c)=\{2k\mid k\in \boldsymbol{Z}\}$$

但是

$$L(a)\neq L(b)\neq L(c)\neq L(a)$$

例 2　证明，主理想环R上的循环模 $M=L(x)$ 的任一子模都是循环模。

解　设N是R—模M的子模．由$N\subseteq M=L(x)$ 可知N中元素y可表为$y=nx$的形式，令

$$A=\{n\in R\mid nx\in N\}$$

易证A是R的理想，由R是主理想环，可知存在 $a\in A$，使

$$A=(a)=\{ra\mid r\in R\}$$

由此得

$$N=\{nx\mid n\in A\}=\{(ra)x\mid r\in R\}=L(ax)$$

即子模N是由模元素ax生成的循环模。

例 3　设M是可换环R上的模。

（1）如果R是整环，则M的所有非自由元集合N是M的子模。

（2）举例说明：如果环R有零因子，则（1）中结论不

一定正确。

解 令M在R上的非自由元集为N。

（1）若$\forall x,y\in N$，则存在$a,b\in R$，使$ax=\theta$，$by=\theta$且$a\neq 0$，$b\neq 0$。由R是整环知：$ab=ba\neq 0$，于是得

$$ab(x-y)=(ab)x-(ab)y=b(ax)-a(by)=\theta$$

故有 $x-y\in N$。

若$\forall\ r\in R,x\in N$，则存在$a\in R$，$a\neq 0$，$ax=\theta$，于是有

$$a(rx)=r(ax)=\theta$$

故有 $rx\in N$。因此知N是M的子模。

（2）例（i）考察环模：$\mathbf{Z}_6$—模$\mathbf{Z}_6$。非自由元集合

$$A=\{\overline{0},\ \overline{2},\ \overline{3},\ \overline{4}\}$$

就不构成子模，这是因为 $\overline{3}-\overline{2}=\overline{1}\notin A$。

例（ii）设 $R=\{(a,b)\mid a,b\in \mathbf{Z}\}$,对于$\forall\alpha=\{a_1,b_1\}$，$\beta=(a_2,b_2)\in R$，规定

$$\alpha+\beta=(a_1+a_2,b_1+b_2),\quad \alpha\cdot\beta=(a_1a_2,b_1b_2)$$

则$(R,\ +,\cdot)$是有$1\neq 0$的交换环。其中

$$1=(1,1),0=(0,\ 0)$$

显然 $\gamma=(1,0)$，$\delta=(0,\ 1)\in R$ 是 R中一对零因子。考查（环模：R—模R的）γ的阶理想

$$O(\gamma)=\{(0,y)\mid\forall y\in \mathbf{Z}\}\neq\{0\}$$

和δ的阶理想

$$O(\delta)=\{(x,0)\mid\forall x\in \mathbf{Z}\}\neq\{0\}$$

所以γ，δ是非自由元，但$\gamma+\delta=(1,\ 1)$是自由元，故非自由元的集合N不能构成M的R—子模。

例 4 令$M=A\oplus B$ 是环R上模M关于子模A和B的直和分解式，证明：商模M/B与A是R—同构的。

解 令 $\varphi: A\to M/B$

$$a\longmapsto\overline{a}=a+B\in M/B,\quad\forall a\in A$$

下面证明φ是模A到模M/B的R—同构映射。

(i) 先证φ是映射

对 $a_1,a_2 \overline{\in} A$，有$\varphi(a_1)=\overline{a}_1,\varphi(a_2)=\overline{a_2}\in M/B$。若$\overline{a}_1 \neq \overline{a}_2$，则 $\overline{a}_1 - \overline{a}_2 = \overline{a_1-a_2} \neq \overline{0}$，故$a_1-a_2 \overline{\in} B$。又因$A\cap B=\{0\}$于是得$a_1\neq a_2$，$\varphi$是映射。

(ii) 再证φ是双射

对 $a_1,a_2\in A$，当$a_1\neq a_2$时，有$a_1-a_2=a\neq 0$，因$A\cap B=\{0\}$故知，$a\in A, a\overline{\in} B$。于是$\overline{a}\neq\overline{0}$。再由$\overline{a}_1-\overline{a}_2=\overline{a}$可知$\overline{a_1}\neq\overline{a}_2$。$\varphi$是单射。

$\forall \overline{x}\in M/B$，则$\overline{x}=x+B$，$x\in M$，再由$M=A\oplus B$可知$x=a+b$，$a\in A$，$b\in B$，于是知$\overline{x}=\overline{a}$，$\varphi(a)=\overline{x}$，故$\varphi$是满射。

(iii) 最后证φ保持运算

对 a_1，$a_2\in A$有

$$\varphi(a_1+a_2)=\overline{a_1+a_2}=\overline{a}_1+\overline{a}_2=\varphi(a_1)+\varphi(a_2)$$

对 $a\in A$，$r\in R$ 有

$$\varphi(ra)=\overline{ra}=r\overline{a}=r\varphi(a)$$

于是断定φ是模A到模M/B的R—同构映射。故

$$A\overset{\varphi}{\cong}M/B$$

例5．令

$R=\{(a_1\ a_2\cdots)\mid a_i\in \mathbf{Z}\ \ i=1,\ 2,\ \cdots\}$，$\forall\alpha=(a_1\ a_2\cdots)$，$\beta=(b_1\ b_2\cdots)\in R$，规定

$$\alpha+\beta=(a_1+b_1\ \ a_2+b_2\cdots),\ \alpha\cdot\beta=(a_1b_1\ \ a_2b_2\cdots)$$

则$\{R;+\ .\}$是有$1\neq 0$的可换环，环模R是循环模，即

$$R=L(1)$$

是有限生成的．试找出模R的一个非有限生成的子模。

解　对元素

$$\alpha=(a_1\cdots a_n\ \ 0\cdots)\in R$$

$a_n \neq 0$,则称 n 为 α 的长度，α 是 R 中长度有限的元素。记为 $l(\alpha)=n$。令

$$A=\{\alpha \in R \mid l(\alpha)=n \in \mathbf{N}\}$$

是 R 中长度有限的元素集合，则 A 是 R 的理想，R—模 A 是 R—模 R 的子模。此子模是无限生成模。事实上，对 A 的任一有限子集 $S=\{\alpha_i\}_{i=1}^m$ 来说，都有非负有限整数集 $\{l(\alpha_i)\}_{i=1}^m$，令其中最大数为 $l(\alpha_k)$，则由 S 生成的环 R 的理想是 A 的子模，(S) 中元素的长度均不超过 $l(\alpha_k)$ 所以 $A \supset (S)$，S 不可能是模 A 的生成集，故断定 A 是无限生成的 R—模，

此例说明：**循环模的子模不一定是循环模；有限生成模的子模不一定是有限生成的。**

第五章　扩域学习指导

一　内容概要

域是一类特殊的环，是第三章所讲的环中条件最强的环。域的理论与方程式根的理论密切相关，读者应复习一下高等代数以及第三章的有关内容。

对于域的研究，在方法上与群论、环论有很大不同。比如在第二章我们看到，研究一个群时，一般的是先讨论这个群的总体性质，然后再来讨论它的子群的性质。现在我们采取与此相反的程序来研究域：对于给定的域，探讨它的各种各样的扩张（扩域）。采取这个做法的原因是基于域论中一个事实：任何一个域，它不是有理数域Q的扩张，便是以素数p为模的剩余类环Z_p的扩张，二者必居其一。而域Q和Z_p的结构是清楚的。也就是说，如果把Q的以及Z_p的所有可能的扩张都研究了，那么就研究了所有的域。域论的内容很丰富，本书不能涉及过多，只讨论几类最基本的扩张：单纯扩张、有限扩张以及它们在多项式的分裂域和有限域上的应用。

二　内容分析

§1　特征数　素域

（一）内容提要

本节是这一章的基础。它告诉我们，每个域都具有唯一确

定的特征数．正如这个概念的名称，特征数确实在很大程度上反映了一个域的特征．特征数相同的域，有着许多相同的性质，特征数不同的域，有着许多不同的性质．这一节还告诉我们，每个域都包含着一个最小的子域——素域，而且从同构角度看，素域只有两种：Q和Z_p．这就从理论上给出了研究域的理论采用研究扩张的方法的依据．值得注意的是，一个域所含的素域是Q还是Z_p，完全由这个域的特征数来决定．所以特征数和素域是域论的两个重要的基本概念．本节主要内容有

1　给出三个基本概念：域的特征数、素域和扩张．

2　围绕特征数概念的主要结果：

（1）　域的加法群中非零元素的阶都相等．当此阶有限时，它必是素数（定理1）；

（2）　域F的特征数为$\infty \Longleftrightarrow$对于$F$中的某个非零元素$a$和任一正整数$n$有 $na \neq 0$；

域F的特征数为$p \Longleftrightarrow$对于F中的某个非零元素a，p是使$pa=0$的最小正整数（推论1）．

3　关于素域的主要结果：

（1）素域的结构定理（定理2）；

（2）任一域都含有唯一的素域．

（二）补充说明

1　关于环的特征数

定理1保证了对域定义特征数的合理性．如果把定理1中的域F改为无零因子环，该定理仍然成立．所以完全可以对无零因子环定义特征数的概念，有的书就是这样做的．另外，有的书把特征数是∞规定为特征数是零，这仅是称呼不同，无本质差别．

2　推论1实质是特征数的一个等价定义，可用它来确定一个域的特征数．大多数场合，利用推论1更为方便．特别是采用$a=1$来确定特征数往往更简捷．

3　读者以往熟习的域（如各种数域）大多数是特征数为

∞的域，它们在性质上与特征数是 p 的域有许多差别。在数域里惯用的一些法则有可能在特征数为 p 的域中不成立，需要特别慎重，避免用错。

4　定理 2 的证明步骤稍微复杂一些，初读不易马上读懂。如果读者能分清步骤、仔细思考，最后一定能清楚地掌握它。类似的证明方法后面还将出现。

5　定理 2 和定理 3 是本节的主要结果，前者说明素域的结构，素域只有两种：Q和R_p；后者表明任何一个域都是一个确定的素域的扩张。两者合起来说明，任一域或者是Q的扩张或者是 Z_p 的扩张。

6　关于域扩张的记号 E/F。它与前几章中商群、商环（差环）的记号相同，但在涵义上有本质区别，E/F 只表示域 E 与域F之间的关系：E 是 F 的扩张，即 F 是 E 的子域。E/F不是一个集合。

§2　扩　　张

（一）内容提要

做为研究域扩张的第一步，本节首先对已知域给出了在一个“大域”的范围内构造扩张的一般方法，即添加。由添加得出扩张不止是方法问题，更重要的是，任何一个扩张都可看做是由添加得到的，而且从添加元素身上可以看到所得到的扩张的性质。所以对添加元素的观察是我们时时应做的事。

其次，本节对所有的扩张，给出一个最基本的分类，分成代数扩张和超越扩张两大类。超越扩张的理论已超出本书范围，将不太涉及，我们讨论的重点是属于代数扩张方面的一些内容。

最后，本节对代数元和最小多项式这两个概念以及它们的性质做了介绍。这些都是研究下一节内容的必备知识。

本节主要内容：

1　给出几个基本概念：添加（也是构选扩张的基本方法）、代数元、超越元、最小多项式、代数扩张和超越扩张。

2　关于添加的性质：

（1）从另一个角度描述添加（命题1）；

（2）在域E的子域F上添加E的一个子集合S，可以把S分成两个或有限个集合逐个添加到F上去（定理1及其推广）。

3　关于代数元和最小多项式的性质：F上的代数元α的最小多项式的$\varphi(x)$唯一性、不可约性以及$\varphi(x)$是F上以α为根的任一多项式的因子（命题2—命题4）。

（二）补充说明

1　命题1是定义1的等价定义。定义1是从$F(S)$与E的同时包含F和S的子域的关系来刻划$F(S)$；而命题1则是从$F(S)$的元素的形式刻划$F(S)$。

命题1指出：

$$F(S)=\left\{\frac{f(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g(\alpha_1,\alpha_2,\cdots,\alpha_n)}\alpha_i\in S,\quad f(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n),\right.$$

$g(\alpha_1,\alpha_2,\cdots,\alpha_n)\neq 0$ 是$\alpha_1,\alpha_2,\cdots,\alpha_n$在$F$上的多项式，$n$是正整数$\}$

显然$f(\alpha_1,\alpha_2,\cdots,\alpha_n)$是$E$的元素，同时$g(\alpha_1,\alpha_2,\cdots,\alpha_n)$是$E$的非零元素。所以有理分式

$$\frac{f(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g(\alpha_1,\alpha_2,\cdots,\alpha_n)}$$

也是E的元素。于是$F(S)$是由下述元素组成：对S中的任意n个元素$\alpha_1,\alpha_2,\cdots,\alpha_n$，取遍它们的所有有理分式。

2　根据定义，如果$\alpha\in F$，则$F(\alpha)=F$。进一步，对于$F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta)$来说，当$\beta$可被$\alpha_1,\alpha_2,\cdots,\alpha_n$在$F$上有理表示（即$\beta$可表成$\alpha_i$的有理分式）时，则可在添加元素中去掉$\beta$，即

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta)=F(\alpha_1\alpha_2,\cdots,\alpha_n)$$

3　关于代数元和超越元的判定

要判定元素 α 是 F 上的代数元，一般方法是找出 F 上以 α 为根的非零多项式（后面将见到，在特殊情况还有其它判定方法）．要判定 α 是 F 上的超越元，一般是用反证法．即假设存在 F 上的非零多项式以 α 为根，由此推出矛盾．

4　关于 F 上代数元 α 的最小多项式的存在性

这是显然的事实．只须对 F 上所有以 α 为根的非零多项式的次数应用自然数最小数原理，即可推得 α 的最小多项式一定存在．

5　关于最小多项式的判定

设 α 是域 F 的扩域中的元素，$\varphi(x)$ 是 F 上的首系数是 1 的多项式，如果能证明 α 是 $\varphi(x)$ 的根，再证明 $\varphi(x)$ 在 F 上是不可约多项式，这样就可断言 $\varphi(x)$ 是 α 在 F 上的最小多项式．

§3　单纯扩张

（一）内容提要

我们已经知道，任何一个扩张都可由添加得到．那么，最简单的扩张自然是添加一个元素的扩张，即单纯扩张．本节将研究单纯扩张的结构，特别是对于添加一个代数元的情形——单纯代数扩张将做更多的讨论．下一节是讨论有限扩张，届时将看到，任一有限扩张可以通过有限次单纯扩张来实现．所以掌握单纯扩张的结构是研究其它扩张必经之路．本节主要内容

1　讲述两个基本概念：单纯代数扩张和单纯超越扩张．

2　单纯扩张的结构定理（定理 1）．

3　单纯代数扩张 $F(\alpha)$ 中元素的最简表达形式以及 $F(x)$ 中元素间的运算法则．

4　对于任一域，单纯扩张的存在性．

（二）补充说明

1　定理 1 是本节的中心结果．其意义，首先在于它清楚

地告诉我们单纯扩张的代数结构：对于任一元素α，当α是F上的超越元时，$F(\alpha)$与$F(x)$等同；当α是F上的代数元时，$F(\alpha)$与$F[x]/(\varphi(x))$等同，其中$\varphi(x)$是α在F上的最小多项式。由于$F(x)$及$F[x]/(\varphi(x))$都是我们已经掌握其结构的具体的域，于是我们对于单纯超越扩张和单纯代数扩张结构的研究即告完成。

定理1的意义还在于，它说明了单纯扩张的唯一性，亦即，对于确定的域F，F的单纯超越扩张只有一个$F(x)$；对于确定的域F和F上的一个首项系数是1的不可约多项式$\varphi(x)$，F只有一个单纯代数扩张$F[x]/(\varphi(x))$，其中$\varphi(x)$是添加元素在F上的最小多项式。结合本节最后部分关于单纯扩张存在性的论述，我们可以得出结论：对于给定的域F，存在而且只存在一个单纯超越扩张；对于给定的域F和F上的首项系数为1的不可约多项式$\varphi(x)$，存在而且只存在一个F的单纯代数扩张，其添加元素的最小多项式是$\varphi(x)$。

2　本节新引入两个扩张：单纯代数扩张和单纯超越扩张。以后还将引入别种类型的扩张。在引入一个新的扩张概念时，读者应留意，它与已讲过的扩张有什么关系。比如单纯超越扩张$F(\alpha)$，由于$F(\alpha)$含有超越元α，所以单纯超越扩张必是上节讲过的超越扩张。同样应该考虑单纯代数扩张$F(\alpha)$是代数扩张，还是超越扩张呢？这要看$F(\alpha)$是否含有F上的超越元，而对这个问题，此刻我们还不能马上回答出来，那就作为悬案，留待以后解决。但应明确，这个问题必须解决。在全章学完时，对于所接触到的各种扩张之间的隶属关系，应该有清楚地了解。

这里还应注意，在确定两种扩张之间的关系时，不要只由扩张的名称便加默认，而不追求从定义出发的严格论证。比如，在下节将证明单纯代数扩张是代数扩张，而不能因为这种扩张的名称中有“代数”字样，就“显然”是代数扩张了事。

3　设α是F上的代数元，其在F上的最小多项式为

$\varphi(x)$。单纯代数扩张 $F(\alpha)$ 的元素的一般形式是

$$\frac{f(\alpha)}{g(\alpha)}, \quad g(\alpha) \neq 0$$

根据定理 2，存在次数小于 n 的 F 上的多项式$h(x)$，使得

$$\frac{f(\alpha)}{g(\alpha)} = h(\alpha)$$

那么，对于给定的$\frac{f(\alpha)}{g(\alpha)}$如何求$h(\alpha)$呢？

上式可表成

$$h(\alpha) = f(\alpha)(g(\alpha))^{-1}$$

这里$g(\alpha)$也是$F(\alpha)$中的元素．因此上述问题就归结为求 α 的多项式 $g(\alpha)$ ($\neq 0$) 的逆元问题．现介绍求 $g(\alpha)$ 的逆元的一般方法．

由于$g(\alpha) \neq 0$，有$\varphi(x) \nmid g(x)$．再因$\varphi(x)$是不可约多项式，得$(g(x),\ \varphi(x)) = 1$．用带余除法必能求得$u(x), v(x)$使

$$g(x)u(x) + \varphi(x)v(x) = 1$$

从而

$$g(\alpha)u(\alpha) = 1, \quad \text{即} u(\alpha) = (g(\alpha))^{-1}$$

例如，设$Q(\alpha)$是Q的单纯代数扩张，α 在Q上的最小多项式为$\varphi(x) = x^2 - x + 1$．试将$Q(\alpha)$中的元素

$$\theta = \frac{\alpha^2 + \alpha + 1}{3\alpha^3 - 2\alpha^2 + \alpha + 2}$$

表为次数小于 2 的 α 的多项式，此处

$$f(\alpha) = \alpha^2 + \alpha + 1, \quad f(x) = x^2 + x + 1$$

$$g(\alpha) = 3\alpha^3 - 2\alpha^2 + \alpha + 2, \quad g(x) = 3x^3 - 2x^2 + x + 2$$

利用带余除法求得$u(x) = x$，$v(x) = -3x^2 - x + 1$使

$$g(x)u(x) + \varphi(x)v(x) = 1$$

于是

$$(g(\alpha))^{-1} = u(\alpha) = \alpha$$

故

$$\theta = f(\alpha)(g(\alpha))^{-1} = (\alpha^2+\alpha+1)\alpha = \alpha^4+\alpha^2+\alpha = q(\alpha)$$

再将$q(\alpha)$化为次数小于 2 的 α 的多项式：以$\varphi(x)$除$q(x) = x^3-x^2+x$得余式$h(x)=2x-2$，则

$$\theta = h(\alpha) = 2\alpha-2$$

4　设$F(\alpha)$和$F(\beta)$是域 F 的单纯扩张，如果 $\alpha\in F(\beta)$ 并且 $\beta\in F(\alpha)$，那么$F(\alpha)=F(\beta)$。

§4　有 限 扩 张

（一）内容提要

本节讨论一类比较广泛的代数扩张——有限扩张，讲述有限扩张的性质。这部分内容与多项式根的理论关系密切。主要内容：

1　给出两个基本概念：有限扩张和无限扩张。

2　有限扩张的次数定理（定理 1 及其推论）。

3　有限扩张必是代数扩张（定理 2）。

4　有限扩张的一个充分必要条件（定理 3）。

（二）补充说明

1　设 E 是 F 的扩张。E 是不是 F 的有限扩张，是由 E 做为 F 上的向量空间时 E 的维数来决定的。当 E 是 F 的有限扩张时，确定扩张次数(E/F)的一个方法，是寻找 E 在 F 上的一组基底，看基底的元素个数。由于证明了 F 的有限扩张与在 F 上添加有限个代数元所得到的扩张的一致性（定理 3），使人容易误认为添加元素的个数就是扩张次数。这是截然不同的两个概念，切不可混淆。

2　由定理3和定理2可直接推得，在 F 上添加有限个代数元所得到的扩张是 F 的代数扩张。这个结果也可推广到更一般情形：设E/F，$S\subseteq E$，S 的每个元素都是 F 上的代数元，则 $F(S)$是 F 的代数扩张。

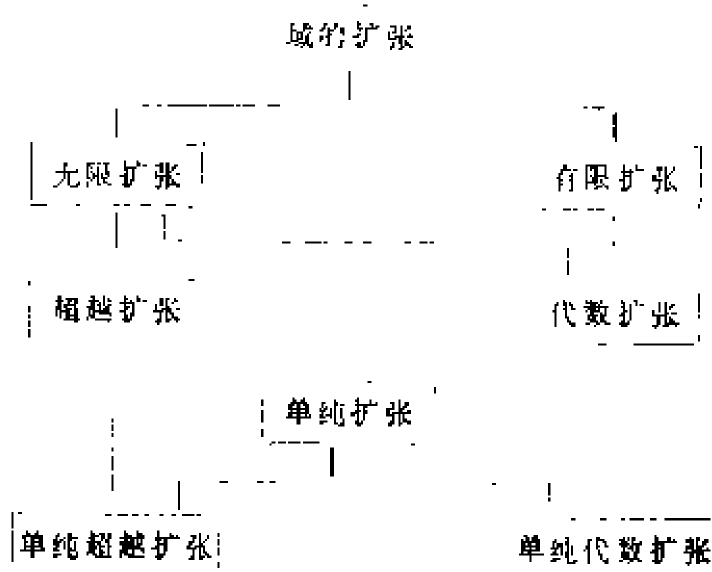
事实上，$\forall\beta\in F(S)$，由 § 2 命题 1 知

$$\beta=\frac{f(\alpha_1,\alpha_2,\cdots,\alpha_n)}{g(\alpha_1,\alpha_2,\cdots,\alpha_n)},\quad \alpha_i\in S,\quad g(\alpha_1,\alpha_2,\cdots,\alpha_n)\neq 0$$

其中 n 是正整数，α_i 都是 F 上的代数元。于是 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是有限扩张，从而是代数扩张。再因 $\beta\in F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，所以 β 是 F 上的代数元。亦即 $F(S)$ 是 F 的代数扩张。

上述论证表明，不找出以 β 为根的多项式有时也能判定 β 是代数元。

3　已讲过的几种扩张之间的关系如下表：



§5　分　裂　域

（一）内容提要

做为有限扩张理论的应用，本节介绍了多项式的分裂域，主要是论证任一域上的 $n(\geqslant 1)$ 次多项式的分裂域的存在性和唯一性。在本书学习指导的开始部分我们说过，伽罗瓦理论全面论述了多项式求解公式的存在性问题。分裂域的概念在伽罗瓦理论中起着重要作用。限于篇幅，我们不能介绍伽罗瓦理论。然而，了解一些分裂域的理论，对提高多项式根的理论的认识是有益的，本节主要内容：

1　给出分裂域和同构开拓两个概念。

2　分裂域的存在性（定理1）。

3　两个域之间的同构映射在它们的多项式环上存在同构开拓（引理1）。

4　分裂域的唯一性（定理2及其推论）。

（二）补充说明

1　定理1的证明，实质上是往F上逐次添加$f(x)$的所有n个根而得到$f(x)$的分裂域。

对于具体的F上的n（$\geqslant$）次多项式$f(x)$，如果能够求出$f(x)$在F的一个扩域中的n个根，那么把这n个根添加到F上便得到$f(x)$的分裂域。

2　对于域F上的$n(\geqslant 1)$次多项式$f(x)$，在第三章§10中已经知道，在F的任一扩域里$f(x)$根的个数不能超过n。本节的分裂域存在性表明，确有F的扩域恰好含有$f(x)$的n个根。而且分裂域的唯一性表明，在$f(x)$的两个不同分裂域里，所含有的$f(x)$的两组根在运算性质上没有区别。因此我们可以认为，对于域F上的n（$\geqslant 0$）次多项式$f(x)$，存在唯一的一组n个根。

3　引理2是说，如果域F与$\widetilde{F}$同构，$\sigma: F\cong\widetilde{F}$，那么它们的单纯代数扩张$F(\alpha)$与$\widetilde{F}(\widetilde{\alpha})$同构，$\sigma': F(\alpha)\cong\widetilde{F}(\widetilde{\alpha})$，其中$\sigma'$是$\sigma$的同构开拓，并且$\sigma'(\alpha)=\widetilde{\alpha}$。此结论成立的前提条件是$\alpha$在$F$上的最小多项式$\varphi(x)$在$\sigma$之下对应着$\widetilde{\alpha}$在$\widetilde{F}$上的最小多项式$\widetilde{\varphi}(x)$。

引理2证明的要点是：首先由§3定理1知，$F(\alpha)$与$F[x]/(\varphi(x))$同构，$\widetilde{F}[x]/(\widetilde{\varphi}(x))$与$\widetilde{F}(\widetilde{\alpha})$同构。其次利用已知条件，$\sigma: F\cong\widetilde{F}$，在$F[x]/(\varphi(x))$与$\widetilde{F}[x]/(\widetilde{\varphi}(x)$之间建立了同构关系。最后由同构关系具有传递性，得到$F(\alpha)$与$\widetilde{F}(\widetilde{\alpha})$同构的结论。并且其同构映射$\sigma'$是$\sigma$的同构开拓，使得$\sigma'(\alpha)=\widetilde{\alpha}$。

在证明过程中，采用了下列记号：

F中的元素a在σ之下的象是$\widetilde{F}$中的元素$\widetilde{a}$。

F上的多项式$f(x)$（即$F[x]$中的元素）在σ之下所对应的

$\widetilde{F}$上的多项式记为$\widetilde{f}(x)$（即$\widetilde{F}[x]$中的元素）。

$F[x]/(\varphi x)$中的元素记为$\overline{f(x)}=f(x)+(\varphi(x))$，它是$F(\alpha)$中的元素$f(\alpha)$在$\sigma_1$之下的象。

$\widetilde{F}[x]/(\widetilde{\varphi}(x))$中的元素记为$\overline{\widetilde{f}(x)}=\widetilde{f}(x)+(\widetilde{\varphi}(x))$，它是$\widetilde{F}(\widetilde{\alpha})$中的元素$\widetilde{f}(\widetilde{\alpha})$在$\sigma_2$之下的原象。

4　定理2是说，假设两个域F和$\widetilde{F}$同构．$\sigma: F\cong\widetilde{F}$，$f(x)$和$\widetilde{f}(x)$分别是$F$和$\widetilde{F}$上的$n(\geqslant)$次多项式，而且它们在$\sigma$之下相对应，那么它们的分裂域$F(\alpha_1, \alpha_2, \cdots, \alpha_n)$和$\widetilde{F}(\widetilde{\alpha_1}, \widetilde{\alpha_2}, \cdots, \widetilde{\alpha_n})$同构，$\sigma': F(\alpha_1, \alpha_2, \cdots, \alpha_n)\cong\widetilde{F}(\widetilde{\alpha_1}, \widetilde{\alpha_2}, \cdots, \widetilde{\alpha_n})$，而且$\sigma'$是$\sigma$的同构开拓，使得$f(x)$的根$\alpha_i$在$\sigma'$之下的象分别是$\widetilde{f}(x)$的根$\widetilde{\alpha_i}$。

5　有的书把分裂域叫做根域或分解域。

§6 有限域

（一）内容提要

本节是利用分裂域的理论讨论有限域．可以这样做的原因是，任一有限域E恰好是Z_p上的多项式$f(x)=x^q-x$的分裂域．其中p和q分别是E的特征数和元素个数．

本节的前一部分是讨论Z_p上h次单位根的性质．这是因为有限域的每个非零元素都是Z_p上的单位根，单位根的理论可以应用到有限域的研究中来．本节主要内容：

1　给出Z_p上h次单位根的概念。

2　Z_p上h次单位根的性质（命题1—3）．其中主要的是Z_p的扩张E如果含有h个h次单位根，那么这些单位根的集合关于E的乘法组成循环群。

3　有限域的性质（定理1—4）．其中主要的是定理2及其推论．即任一有限域都是$f(x)=x^q-x$在Z_p上的分裂域，其中q和p分别是该域的元素个数和特征数；元素个数相等的两个有限域必同构。

4　有限域的结构定理：每个有限域都是它所含素域的单

纯代数扩张（定理 4 的推论）。

（二）补充说明

1　应注意 Z_p 上 h 次单位根定义中对 h 的要求条件：h 是与 p 互素的正整数。对于不满足这个条件的 h 是得不到有关结果的。

2　定理 1 说明，任何一个有限域 E，其元素个数 q 必是一个素数的正整数次幂。由于整数的标准分解式是唯一确定的，所以 E 的特征数 p 以及 E 做为 Z_p 的有限扩张的扩张次数 n 都由 q 所唯一确定。求 E 的特征数 p 和 E 所含的素域 Z_p 以及扩张次数 n，可由求 q 的标准分解式而全部得到。

进而由定理 1 的推论知，元素个数相同的有限域具有完全相同的代数性质。所以有限域的代数性质由该域的元素个数所完全确定。

3　对于有限域，除本书正文部分所给出的结果之外，还有许多有趣性质，这里再介绍两个。

（1）设 E 是特征数为 p 的有限域，则 E 的每个元素的 p 次方根属于 E。

证　设 E 的元素个数为 q，F 是 E 的所有元素的 p 次幂的集合：$F=\{a\in E|a=\alpha^p,\alpha\in E\}$。显然$F\subseteq E$。

我们说，对于 E 中不同的元素 α,β，必有$\alpha^p\neq\beta^p$。否则由

$$\alpha^p=\beta^p$$

得

$$\alpha_p-\beta_p=0,\ (\alpha-\beta)^p=0,\ \alpha-\beta=0,\ \alpha=\beta$$

因此，F 的元素个数也是 q，由此得 $F=E$。从而 $\forall a\in E$，有 $a\in F$，故$a=\alpha^p$，$\alpha\in E$。　　证完。

（2）有限域的任一有限扩张都是单纯代数扩张。

证　设 F 是特征数为 p 的 q 元有限域，E 是 F 的 n 次扩张。则 E 也是特征数为 p 的有限域，其元素个数为q^n。由定理 4 推论知，E 是其素子域 Z_p 的单纯代数扩张

$$F=Z_p(\alpha)$$

而素域Z_p也是F的子域，所以

$$Z_p(\alpha)\subseteq F(\alpha)$$

从而

$$E=F(\alpha)$$

证完。

三 例题选讲

例 1 求$\frac{2i+1}{i-1}$在Q上的最小多项式，并问$Q\left(\frac{2i+1}{i-1}\right)$与$Q(i)$是否相同？

解 令

$$\alpha=\frac{2i+1}{i-1}=\frac{1}{2}-\frac{3}{2}i$$

α的共轭复数为

$$\overline{\alpha}=\frac{1}{2}+\frac{3}{2}i$$

于是

$$f(x)=(x-\alpha)(x-\overline{\alpha})=x^2-x+\frac{5}{2}$$

是以α和$\overline{\alpha}$为根的二次有理系数多项式。显然$f(x)$在Q上不可约，所以$f(x)$是α在Q上的最小多项式。容易看出

$$i\in Q\left(\frac{1}{2}-\frac{3}{2}i\right)$$

及

$$\frac{1}{2}-\frac{3}{2}i\in Q(i)$$

故

$$Q(i)=Q\left(\frac{1}{2}-\frac{3}{2}i\right)=Q\left(\frac{2i+1}{i-1}\right)$$

例 2 设$E_1=Q\left(2^{\frac{1}{4}},\ 2^{\frac{1}{4}}i\right)$，$E_2=Q\left(2^{\frac{1}{3}},\ 2^{\frac{1}{3}}\omega\right)$，其中$\omega=\frac{-1+\sqrt{3}i}{2}$。证明

$$(E_1/Q(2^{\frac{1}{3}}))=2,\quad (E_1/Q)=6$$
$$(E_2/Q(2^{\frac{1}{3}}))=4,\quad (E_2/Q)=12$$

证明 考虑 $Q(2^{\frac{1}{3}})$。$2^{\frac{1}{3}}$在 Q 上的最小多项式为 x^3-2，所以

$$(Q(2^{\frac{1}{3}})/Q)=3$$

其次

$$E_1=Q(2^{\frac{1}{3}},\ 2^{\frac{1}{3}}i)=Q(2^{\frac{1}{3}})(2^{\frac{1}{3}}i)=Q(2^{\frac{1}{3}})(i)$$

i 在$Q(2^{\frac{1}{3}})$上的最小多项式为 x^2+1，所以

$$(E_1/Q(2^{\frac{1}{3}}))=(Q(2^{\frac{1}{3}})(i)/Q(2^{\frac{1}{3}}))=2$$

进而

$$(E_1/Q)=(E_1/Q(2^{\frac{1}{3}}))\ (Q(2^{\frac{1}{3}})/Q)=2\times3=6$$

再者

$$E_2=Q(2^{\frac{1}{3}},\ 2^{\frac{1}{3}}\ \omega i)=Q(2^{\frac{1}{3}})(2^{\frac{1}{3}}\omega_i)=Q(2^{\frac{1}{3}})(\omega i)$$

现在我们来证明

$$Q(2^{\frac{1}{3}})(\omega i)=Q(2^{\frac{1}{3}})(\omega,i) \qquad (1)$$

事实上，显然 $\omega i\in Q(2^{\frac{1}{3}})(\omega,i)$。另一方面，由$\omega^3=1$，有

$$Q(2^{\frac{1}{3}})(\omega i)\ni-(\omega i)^3=i,Q(2^{\frac{1}{3}})(\omega i)\ni(\omega i)^4=\omega$$

故（1）式成立。于是

$$E_2=Q(2^{\frac{1}{3}})(\omega,\ i)=Q(2^{\frac{1}{3}})(\omega)(i)$$

而ω在 $Q(2^{\frac{1}{3}})$上的最小多项式为x^2+x+1，故

$$(Q(2^{\frac{1}{3}})(\omega)/Q(2^{\frac{1}{3}}))=2$$

i 在 $Q(2^{\frac{1}{3}})(\omega)$上的最小多项式为$x^2+1$，故

$$(Q(2^{\frac{1}{3}})(\omega)(i)/Q(2^{\frac{1}{3}})(\omega))=2$$

于是

$$(E_2/Q(2^{\frac{1}{3}}))=(Q(2^{\frac{1}{3}})(\omega)(i)/Q(2^{\frac{1}{3}})(\omega))(Q(2^{\frac{1}{3}})\cdot(\omega)/Q(2^{\frac{1}{3}}))=2\times2=4$$

而

$$(E_2/Q)=(E_2/Q(2^{\frac{1}{3}}))\ (Q(2^{\frac{1}{3}})/Q)=4\times3=12$$

例 3 设$(K/Q)=2$。（1）证明：$K=Q(\sqrt{a})$，其中 a

是无素数平方约数的整数；（2）设 b 也是无素数平方约数的整数，证明：当 $a\neq b$ 时，则 $Q(\sqrt{a})\neq Q(\sqrt{b})$.

证明 （1）由 $(K/Q)=2$ 知，K 必含有非有理数 d（否则 $K=Q$，则有 $(K/Q)=1$）。考虑 $Q(d)$. 由于 $Q\subseteq Q(d)\subseteq K$，则根据§4定理1有

$$(K/Q(d))(Q(d)/Q)=K/Q=2$$

其中 $(Q(d)/Q)\neq 1$（否则可推得 $d\in Q$），只有 $(Q(d)/Q)=2$，于是 $(K/Q(d))=1$，故 $K=Q(d)$.

另一方面，由§4命题，d 在 Q 上的最小多项式 $\varphi(x)$ 是二次的. 设

$$\varphi(x)=x^2+bx+c,\quad b,c\in Q$$

用 b，c 的分母的最小公倍乘 $\varphi(x)$，得到整系数多项式

$$f(x)=lx^2+mx+n$$

由于 $f(x)$ 和 $\varphi(x)$ 具有相同的根，故 d 是 $f(x)$ 的根。不妨令

$$d=\frac{-m+\sqrt{m^2-4ln}}{2l}$$

其中 m^2-4ln 是整数. 因为 d 不是有理数，所以 m^2-4ln 不能是非负的完全平方数. 于是 m^2-4ln 可表成

$$m^2-4ln=k^2\cdot a$$

其中 k 是非负整数，a 是不含素数平方约数的整数，故

$$\sqrt{m^2-4ln}=k\sqrt{a}$$

于是有

$$K=Q(d)=Q\left(\frac{-m+\sqrt{m^2-4ln}}{2l}\right)$$

$$=Q\left(\frac{-m+k\sqrt{a}}{2l}\right)=Q\sqrt{a}\cdot$$ （1）得证.

（2）设 b 也是无素数平方约数的整数.

如果 $b=1$，则因 $\sqrt{a}\neq\sqrt{b}=1$，有 $Q(\sqrt{a})\neq Q=(Q\sqrt{b})$.

如果 $b\neq 1$，假设 $Q(\sqrt{b})=Q(\sqrt{a})$，则 $\sqrt{b})\in Q(\sqrt{a})$.
由于 1，$\sqrt{a}$ 是 $Q(\sqrt{a})/Q$ 的基底，可将 $\sqrt{b}$ 用 1，$\sqrt{a}$ 线性表示

$$\sqrt{b}=r+s\sqrt{a},\ r,\ s\in Q$$

进而

$$b=r^2+s^2a+2rs\sqrt{a} \qquad (※)$$

由于 b 是整数，则必有

$$rs=0$$

其中 s 不能等于零，否则有 $b=r^2$，此时 r 是整数．因 $b\neq 1$，则 $r\neq\pm 1$，故 r 必有素约数，从而 b 有素数平方约数，与题设矛盾．所以 $s\neq 0$，而 $r=0$．于是（※）式化为

$$b=s^2a$$

把 s 表为既约分数 $s=\frac{v}{u}$，则

$$b=\frac{v^2}{u^2}a,\quad u^2b=v^2a$$

由 $(u,v)=1$ 有

$$u^2|a,\ v^2|b$$

因为 a,b 都无素数平方约数，所以 $u^2=v^2=1$，从而

$$a=b$$

与题设 $a\neq b$ 相矛盾．因此 $Q(\sqrt{a})\neq Q(\sqrt{b})$．（2）得证．

例 4 求 $f(x)=x^3-2$ 在 Q 上的分裂域．

解 先求 $f(x)$ 的所有根．由 n 次方根的性质知，只须求出 $f(x)$ 的一个根 α 和所有三次单位根 ω^0,ω,ω^2，则 $\omega^0\alpha,\omega\alpha,\omega^2\alpha$ 即为 $f(x)$ 的所有根．三次单位根是

$$\omega^0=1,\quad \omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i,\quad \omega^2=-\frac{1}{2}-\frac{\sqrt{3}}{2}i$$

而 $x=\sqrt[3]{2}$ 是 $f(x)$ 的一个根．所以 $f(x)=x^3-2$ 的三个根为

$$x_1=\omega^0\sqrt[3]{2}=\sqrt[3]{2}$$

$$x_2=\omega\sqrt[3]{2}=\sqrt[3]{2}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)$$

$$x_3=\omega^2\sqrt[3]{2}=\sqrt[3]{2}\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)$$

因为x_1, x_2, x_3与$\sqrt[3]{2}$，$\sqrt{3}i$可互相有理表出，所以$f(x)$在Q上的分裂域为

$$Q(x_1, x_2, x_3) = Q(\sqrt[3]{2}, \sqrt{3}i)$$

例 5 证明：任一有限域必存在不等于它自身的代数扩张。

证明 设F是q个元素的有限域。我们来寻找F上次数大于1的不可约多项式。因为$\forall a \in F$总有

$$a^q - a = 0$$

所以多项式

$$f(x) = x^q - x + 1$$

在F中无根，从而它在F上的素因式的次数大于1，设$\varphi(x)$是$f(x)$的素因式，β是$\varphi(x)$的一个根。由于$\varphi(x)$的次数大于1，故$\beta \overline{\in} F$。于是F的代数扩张。

$$F(\beta) \supset F$$

第三部分　近世代数习题解答

第一章　基本概念习题解答

§1

1　**解**　$A\cap B=\{2,4\}$，$A\cup B=\{1,2,3,4,6,8\}$，$A\backslash B=\{1,3\}$，$B\backslash A=\{6,8\}$，C在A和B中的补集分别为$\{1,3\}$和$\{6,8\}$。

2　**证**　（1）因为$\forall a\in A\cap A$有$a\in A$，同时$\forall b\in A$有$b\in A\cap A$，所以

$$A\cap A=A$$

因为$\forall a\in A\cup A$有$a\in A$，同时$\forall b\in A$有$b\in A\cup A$，所以

$$A\cup A=A$$

（2）先证第一个等式。$\forall a\in(A\cap B)\cap C$，有$a\in A\cap B$且$a\in C$。由前者知$a\in A$且$a\in B$，于是$a\in B\cap C$，从而$a\in A\cap(B\cap C)$。另一方面$\forall b\in A\cap(B\cap C)$，有$b\in A$且$b\in B\cap C$，由后者知$b\in B$且$b\in C$，于是$b\in A\cap B$，从而$b\in(A\cap B)\cap C$。综上所述得

$$(A\cap B)\cap C=A\cap(B\cap C)$$

再证第二个等式，$\forall a\in(A\cup B)\cup C$，有$a\in A\cup B$或者$a\in C$，于是$a\in A$或者$a\in B$或者$a\in C$。从而$a\in A$或$a\in B\cup C$，得$a\in A\cup(B\cup C)$。另一方面，$\forall b\in A\cup(B\cup C)$有$b\in A$或者$b\in B\cup C$，于是$b\in A$或者$b\in B$或者$b\in C$，从而$b\in A\cup B$或者$b\in C$，得$b\in(A\cup B)\cup C$。综上所述有

$$(A\cup B)\cup C=A\cup(B\cup C)$$

（3） $\forall a\in A\cap B$，有$a\in A$且$a\in B$，即 $a\in B$ 且 $a\in A$，得 $a\in B\cap A$；另一方面，$\forall b\in B\cap A$，有$b\in B$且$b\in A$，得$b\in A\cap B$。故

$$A\cap B=B\cap A$$

$\forall a\in A\cup B$，有$a\in A$或者$a\in B$，即$a\in B$或$a\in A$，得$a\in B\cup A$；另一方面，$\forall b\in B\cup A$，有$b\in B$或$b\in A$，得$b\in A\cup B$。故

$$A\cup B=B\cup A$$

（4） 第一个等式的证明在本章例题选讲中给出。现证第二个等式。

$\forall a\in A\cup(B\cap C)\Longrightarrow a\in A$或$a\in B\cap C\Longrightarrow a\in A$，或者$a\in B$且$a\in C\Longrightarrow a\in A$或$a\in B$，并且$a\in A$或$a\in C\Longrightarrow a\in A\cup B$ 并且 $a\in A\cup C\Longrightarrow a\in(A\cup B)\cap(A\cup C)$。

另一方面，$\forall b\in(A\cup B)\cap(A\cup C)\Longrightarrow b\in A\cup B$并且 $b\in A\cup C\Longrightarrow b\in A$ 或 $b\in B$，并且 $b\in A$ 或 $b\in C\Longrightarrow b\in A$，或者 $b\in B$且$b\in C\Longrightarrow b\in A\cap(B\cap C)$。

综上所述得

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$$

（5） $\forall a\in A\cup(A\cap B)\Longrightarrow a\in A$ 或 $a\in A\cap B\Longrightarrow a\in A$。另一方面，$\forall b\in A\Longrightarrow b\in A$或$b\in A\cap B\Longrightarrow b\in A\cup(A\cap B)$。故 $A\cup(A\cap B)=A$

$\forall a\in A\cap(A\cup B)\Longrightarrow a\in A$，另一方面，$\forall b\in A\Longrightarrow b\in A\cup B\Longrightarrow b\in A\cap(A\cup B)$。故$A\cap(A\cup B)=A$。

§ 2

1 **解** 令

$$\varphi_1:\ 0\longmapsto a,\ 1\longmapsto b,\quad \varphi_2:\ 0\longmapsto b,\ 1\longmapsto a$$

$$\varphi_3:\ 0,1\longmapsto a,\quad \varphi_4:\ 0,1\longmapsto b$$

因为对于A的每个元素，在B中取象的可能共有二种，而且A的

元素个数为 2，所以总共可建立$2\times 2=4$个映射。其中φ_1、φ_2是双射，φ_3、φ_4是非单非满的。

2　证　设$A\xrightarrow{\psi}B\xrightarrow{\varphi}C$。先证本题第一个结论。设$\psi$是单射，则$\forall a,b\in A$，$a\neq b$有$\psi(a)\neq\psi(b)$。由于$\varphi$是单射，得

$$\varphi(\psi(a))\neq\varphi(\psi(b))$$

即

$$\varphi\psi(a)\neq\varphi\psi(b)$$

说明$\varphi\psi$是单射。反之，设$\varphi\psi$是单射，则$\forall a,b\in A$，$a\neq b$有$\varphi\psi(a)\neq\varphi\psi(b)$，即

$$\varphi(\psi(a))\neq\varphi(\psi(b))$$

由于φ是映射，知

$$\psi(a)\neq\psi(b)$$

这说明ψ是单射。因此ψ是单射$\Longleftrightarrow\varphi\psi$是单射。

再证第二个结论。设ψ是满射，$\forall a''\in C$，由于φ是满射，存在$a'\in B$，使得$\varphi(a')=a''$。再由于ψ是满射，则存在$a\in A$，使得$\psi(a)=a'$。于是

$$\varphi\psi(a)=\varphi(\psi(a))=\varphi(a')=a''$$

说明$\varphi\psi$是满射。反之，设$\varphi\psi$是满射，$\forall b'\in B$，令$\varphi(b')=b''\in C$，于是存在$b\in A$使得$\varphi\psi(b)=b''$。而

$$\varphi(\psi(b))=\varphi\psi(b)=b''=\varphi(b')$$

由φ是单射知

$$\psi(b)=b'$$

这说明ψ是满射。

综上所述，ψ是满射$\Longleftrightarrow\varphi\psi$是满射。

3　证　设$A\xrightarrow{\psi}B$，$A'\xrightarrow{\psi'}B'$，$C\xrightarrow{\varphi}D$。由于$\varphi\psi$和$\varphi\psi'$有意义，则

$$B=B'=C$$

由于$\varphi\psi=\varphi\psi'$，则

$$A = A'$$

所以ψ和ψ'都是A到B的映射．其次 $\forall a \in A$，有

$$\varphi\psi(a) = \varphi\psi'(a), \quad \varphi(\psi(a)) = \varphi(\psi'(a))$$

由于φ是单射，得

$$\psi(a) = \psi'(a)$$

故$\psi = \psi'$．

4． 解

$$S_3: \varphi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \varphi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \varphi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\varphi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \varphi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \varphi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

由于φ_1是$\{1,2,3\}$的恒等变换，所以 $\varphi_1\varphi_i = \varphi_i\varphi_1 = \varphi_i$，$i = 1, 2, \cdots, 6$．其余的合成如下：

$$\varphi_2\varphi_2 = \varphi_1, \quad \varphi_2\varphi_3 = \varphi_6, \quad \varphi_2\varphi_4 = \varphi_5, \varphi_2\varphi_5 = \varphi_4, \quad \varphi_2\varphi_6 = \varphi_3,$$

$$\varphi_3\varphi_2 = \varphi_5, \quad \varphi_3\varphi_3 = \varphi_1, \quad \varphi_3\varphi_4 = \varphi_6, \varphi_3\varphi_5 = \varphi_2, \quad \varphi_3\varphi_6 = \varphi_4,$$

$$\varphi_4\varphi_2 = \varphi_6, \quad \varphi_4\varphi_3 = \varphi_5, \quad \varphi_4\varphi_4 = \varphi_1, \varphi_4\varphi_5 = \varphi_3, \quad \varphi_4\varphi_6 = \varphi_2,$$

$$\varphi_5\varphi_2 = \varphi_3, \quad \varphi_5\varphi_3 = \varphi_4, \quad \varphi_5\varphi_4 = \varphi_2, \varphi_5\varphi_5 = \varphi_6, \quad \varphi_5\varphi_6 = \varphi_1,$$

$$\varphi_6\varphi_2 = \varphi_4, \quad \varphi_6\varphi_3 = \varphi_2, \quad \varphi_6\varphi_4 = \varphi_3, \varphi_6\varphi_5 = \varphi_1, \quad \varphi_6\varphi_6 = \varphi_5,$$

§ 3

1 证 $\forall (x, y), (x', y'), (x'', y'') \in \mathbf{R} \times \mathbf{R}$,

（1）因 $x - x = y - y = 0 \in Z$，故$(x, y) \sim (x, y)$．

（2）假设$(x, y) \sim (x', y')$，则$x - x'$，$y - y' \in Z$．由于整数的相反数仍是整数，故$x' - x$，$y' - y \in Z$，即$(x'y') \sim (x, y)$．

（3） 假设$(x, y) \sim (x', y')$，$(x', y') \sim (x'', y'')$，则．$x - x'$，$y - y'$，$x' - x''$，$y' - y'' \in Z$．由于二整数之和仍是整数，故

$$(x - x') + (x' - x'') = x - x'' \in Z$$

$$(y-y')+(y'-y'')=y-y''\in Z$$

即 $(x,y)\sim(x'',y'')$

综上所述，～是 $R\times R$ 的等价关系。

2　证 $\forall a,b,c\in R$，有

（1）$a=a$；（2）当 $a=b$ 时则 $b=a$；（3）当 $a=b$，$b=c$，则 $a=c$。故"="是 R 的等价关系。

$\forall a\in R$，设 $\overline{a}=\{x\in R\mid x=a\}$，显然 $\overline{a}=\{a\}$。故"="所决定的商集为 $Q=\{\{a\}\mid a\in R\}$。

3　解 Z_4 恰含有四个元素：$\overline{0}$，$\overline{1}$，$\overline{2}$，$\overline{3}$。它是 Z 的一个商集。设～是由 Z_4 决定的 Z 的等价关系，则 $\forall a,b\in Z$：

$$a\sim b\Longleftrightarrow a,b\in\overline{i}\in Z_4\Longleftrightarrow a=4g+i,\ b=4q+i,\ g,\ q\in Z$$

即～是以 4 为模的同余关系。

4　解　先给出 A 的一个商集，设 $S_1=\{a,b,c\}$，$S_2=\{d,e\}$，则 $Q=\{S_1,S_2\}$ 是 A 的一个商集。设～是 Q 所决定的 A 的等价关系，则 $\forall x,y\in A$：

$$x\sim y\Longleftrightarrow x,y\in S_i,\quad i=1\text{或}2$$

这样便得到 A 的一个等价关系～。

5　解 $\forall x,y\in A$，定义

$$\sim: x\sim y\Longleftrightarrow x\neq a\text{且}y\neq a$$

～显然是 A 的一个关系，而且～具有对称性和传递性，事实上，$\forall x,y,z\in A$，当 $x\sim y$，则 $x\neq a$ 且 $y\neq a$，故 $y\sim x$；当 $x\sim y$，$y\sim z$，则 $x\neq a$，$y\neq a$，$z\neq a$，故 $x\sim z$。但～不具有反身性。$a\nsim a$。

§ 4

1　解　通过造 $\circ_1$ 和 $\circ_2$ 的运算表来定义 $\circ_1$，$\circ_2$。本题对 $\circ_1$ 和 $\circ_2$ 不要求任何附加条件，所以在表的乘积部分任意填上 A 的元素便可。如定义

$\circ_1$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$\circ_2$	a	b	c	d
a	a	a	a	a
b	a	a	a	a
c	a	a	a	a
d	a	a	a	a

则$\{A; \circ_1, \circ_2\}$是代数体系。

2　解　$\{1,2,3,4\}$共有：1个1阶轮换（1）；$\frac{A_4^2}{2}=6$个2阶轮换：(12),(13),(14),(23),(24),(34)；$\frac{A_4^3}{3}=8$个3阶轮换：(123),(132),(124),(142),(134),(143),(234),(243)；$\frac{A_4^4}{4}=6$个4阶轮换：(1234),(1243),(1324),(1342),(1423),(1432)，以上21个元素都是S_4的元素，此外S_4还有3个元素：(12)(34),(13)(24),(14)(23).令$\varphi_1=(1)$，$\varphi_2=(1234)$，$\varphi_3=(13)(24)$，$\varphi_4=(1432)$，则A的乘法表如下

$\circ$	φ_1	φ_2	φ_3	φ_4
φ_1	φ_1	φ_2	φ_3	φ_4
φ_2	φ_2	φ_3	φ_4	φ_1
φ_3	φ_3	φ_4	φ_1	φ_2
φ_4	φ_4	φ_1	φ_2	φ_3

3　解　$Z_5=\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$，其加法表和乘法表分别为

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

§5

1　**证**　由例2知$\{\boldsymbol{Z};\ \cdot\}\sim\{\boldsymbol{Z}_3;\cdot\}$，如果能证明$\{\boldsymbol{Z}_3;\ \cdot\}\sim\{\{-1,0,1\};\cdot\}$，则由命题1便得到本题的结论．令

$$\varphi:\ \overline{0}\longmapsto 0,\ \overline{1}\longmapsto 1,\ \overline{2}\longmapsto -1$$

则φ是$\boldsymbol{Z}_3$到$\{-1,0,1\}$的满射，而且$\forall x,y\in \boldsymbol{Z}_3$有

$$\varphi(xy)=\varphi(x)\varphi(y)$$

事实上，当x,y中有$\overline{0}$时，则$\varphi(x),\varphi(y)$中必有0，于是

$$\varphi(xy)=\varphi(\overline{0})=0=\varphi(x)\varphi(y)$$

当x，y中有$\overline{1}$时，不失一般性，可设 $x=\overline{1}$，则 $\varphi(x)=\varphi(\overline{1})=1$，于是

$$\varphi(xy)=\varphi(y)=1\cdot\varphi(y)=\varphi(x)\varphi(y)$$

当$x=y=\overline{2}$时，则$\varphi(x)=\varphi(y)=-1$，于是

$$\varphi(xy)=\varphi(\overline{2}\cdot\overline{2})=\varphi(\overline{1})=1=(-1)\cdot(-1)$$
$$=\varphi(x)\varphi(y)$$

综上所述得

$$\varphi:\{Z_3;\ \cdot\}\sim\{\{-1,0,1\};\ \cdot\}$$

再由例 2 和命题 1 知

$$\{Z;\ \cdot\}\sim\{\{-1,0,1\};\ \cdot\}$$

2　证　令

$$\varphi: 1,\ -1\longmapsto 1;\ i,\ -i\longmapsto -1$$

则 φ 是 A 到 B 的满射.其次证明$\forall x,y\in A$:

$$\varphi(xy)=\varphi(x)\varphi(y)$$

当x，y中有 1 或 -1时，不失一般性，可设$x=1$或$x=-1$，则$\varphi(x)=1$．由 φ 的定义知，$\varphi(y)=\varphi(-y)$，于是

$$\varphi(xy)=\varphi(y)=1\cdot\varphi(y)=\varphi(x)\varphi(y)$$

当x,y中无 1 和 -1时，则 $\varphi(x)=\varphi(y)=-1$，而且 $xy=1$ 或-1，于是

$$\varphi(xy)=1=(-1)\cdot(-1)=\varphi(x)\varphi(y)$$

故

$$\varphi:\ \{A;\ \cdot\}\sim\{B;\ \cdot\}$$

3　证　$\forall(a_1,a_2,a_3,a_4)\in V_4$，令

$$\varphi:(a_1,a_2,a_3,a_4)\longmapsto\begin{pmatrix}a_1 & a_2\\ a_3 & a_4\end{pmatrix}$$

则 φ 是V_4到$M_2(F)$的双射，而且$\forall(a_1,a_2,a_3,a_4)$，$(b_1,b_2,b_3,b_4)\in V_4$有

$$\varphi((a_1,a_2,a_3,a_4)+(b_1,b_2,b_3,b_4))$$
$$=\varphi((a_1+b_1,a_2+b_2,a_3+b_3,a_4+b_4))$$

$$=\begin{pmatrix}a_1+b_1 & a_2+b_2\\ a_3+b_3 & a_4+b_4\end{pmatrix}=\begin{pmatrix}a_1 & a_2\\ a_3 & a_4\end{pmatrix}+\begin{pmatrix}b_1 & b_2\\ b_3 & b_4\end{pmatrix}$$

$$=\varphi((a_1,a_2,a_3,a_4))+\varphi((b_1,b_2,b_3,b_4))$$

故

$$\varphi\{V_4;\ +\}\cong\{M_2(F);\ +\}$$

4 解 假设φ是$\{Z_3;\ +\}$的任一自同构，考虑$\varphi(\overline{0})$。由于$\forall x\in Z_3$有

$$\varphi(\overline{0})+\varphi(x)=\varphi(\overline{0}+x)=\varphi(x)$$

故

$$\varphi(\overline{0})=\overline{0}$$

满足此条件的Z_3的双变换共有两个，一个是恒等变换I_{Z_3}，它显然是Z_3的一个自同构。另一个是

$$\eta:\overline{0}\longmapsto\overline{0},\quad \overline{1}\longmapsto\overline{2},\quad \overline{2}\longmapsto\overline{1}$$

现证明η也是Z_3的自同构.只须证$\forall x,y\in Z_3$有

$$\eta(x+y)=\eta(x)+\eta(y)$$

当x,y中有$\overline{0}$时，不失一般性可设 $x=\overline{0}$，则

$$\eta(x+y)=\eta(\overline{0}+y)=\eta(y)=\overline{0}+\eta(y)=\eta(\overline{0})+\eta(y)$$
$$=\eta(x)+\eta(y)$$

当$x=y=\overline{1}$时，则

$$\eta(\overline{1}+\overline{1})=\eta(\overline{2})=\overline{1}=\overline{2}+\overline{2}=\eta(\overline{1})+\eta(\overline{1})$$

当$x=y=\overline{2}$时，则

$$\eta(\overline{2}+\overline{2})=\eta(\overline{1})=\overline{2}=\overline{1}+\overline{1}=\eta(\overline{2})+\eta(\overline{2})$$

当 x,y中一个是$\overline{1}$另一个是$\overline{2}$时，则$\varphi(x),\varphi(y)$ 中一个是$\overline{2}$另一个是$\overline{1}$，此时有

$$\varphi(x+y)=\varphi(\overline{0})=\overline{1}+\overline{2}=\varphi(x)+\varphi(y)$$

综上所述，η保持加法运算，从而η是Z_3的自同构。总之

$\{Z_3;\ +\}$共有两个自同构：I_{z_3}和η。

§6

1 解　根据要求条件，定义$\circ_1$和$\circ_2$分别如下两个表：

$\circ_1$	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

$\circ_2$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

其中$\circ_1$满足交换律，A关于$\circ_2$具有恒等元a。$\circ_1$的表的乘积部分对于主对角线对称；$\circ_2$的表的乘积部分有一行(第一行)和同一列（第一列）分别与表的边行和边列相同。

2 解　我们已经知道$\{Z_4;\ +\}$是交换亚群，只要所定义的运算$\circ$使得$\{Z_4;\ +\}\simeq\{A;\ \circ\}$，那么$\{A;\ \circ\}$便是交换亚群。为此，首先建立$Z_4$到$A$的双射

$$\varphi:\bar{0}\longmapsto a,\quad \bar{1}\longmapsto b,\quad \bar{2}\longmapsto c,\quad \bar{3}\longmapsto d$$

其次，按Z_4的加法去定义A的乘法：$\forall x,y\in A$，存在$x',y'\in Z_4$，使得$\varphi(x')=x$，$\varphi(y')=y$，规定A的乘法为

$$\circ: x\circ y=\varphi(x'+y')$$

具体来说，对应着Z_4的加法表

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

(1)

得到A的乘法表

$\circ$	$\varphi(\overline{0})$	$\varphi(\overline{1})$	$\varphi(\overline{2})$	$\varphi(\overline{3})$
$\varphi(\overline{0})$	$\varphi(\overline{0})$	$\varphi(\overline{1})$	$\varphi(\overline{2})$	$\varphi(\overline{3})$
$\varphi(\overline{1})$	$\varphi(\overline{1})$	$\varphi(\overline{2})$	$\varphi(\overline{3})$	$\varphi(\overline{0})$
$\varphi(\overline{2})$	$\varphi(\overline{2})$	$\varphi(\overline{3})$	$\varphi(\overline{0})$	$\varphi(\overline{1})$
$\varphi(\overline{3})$	$\varphi(\overline{3})$	$\varphi(\overline{0})$	$\varphi(\overline{1})$	$\varphi(\overline{2})$

=

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

由于φ是双射，并且由（1）知，$\forall x', y' \in Z_4$有

$$\varphi(x'+y')=\varphi(x')\circ\varphi(y')$$

故$\varphi:\{Z_4+\}\simeq\{A;\ \circ\}$。由定理3和定理4知$\{A;\ \circ\}$是交换亚群。

3　**证**　先证“$\circ$”满足结合律。$\forall a,b,c\in R$：

$$\begin{aligned}(a\circ b)\circ c&=(a+b-ab)\circ c=a+b-ab+c-(a+b-ab)c\\&=a+b+c-ab-ac-bc+abc\end{aligned}$$

$$\begin{aligned}a\circ(b\circ c)&=a\circ(b+c-bc)=a+b+c-bc-a(b+c-bc)\\&=a+b+c-ab-ac-bc+abc\end{aligned}$$

故

$$(a\circ b)\circ c=a\circ(b\circ c)$$

其次验证R关于运算“$\circ$”有恒等元。事实上，$0\in R$是恒等元：$\forall a\in R$有

$$0\circ a=a\circ 0=a+0-a\cdot 0=a$$

综上所述，$\{R; \circ\}$是亚群。

4 证 用反证法。假设

$$\varphi:\{R;\ +\}\cong\{Z;\ +\}$$

则对于$1\in Z$，应有 $a\in R$ 使得 $\varphi(a)=1$，由于$\frac{a}{2}\in R$，则应有 $n\in Z$使$\varphi\left(\frac{a}{2}\right)=n$。

于是

$$2n=\varphi\left(\frac{a}{2}\right)+\varphi\left(\frac{a}{2}\right)=\varphi\left(\frac{a}{2}+\frac{a}{2}\right)=\varphi(a)=1$$

得 $n=\frac{1}{2}$.但$\frac{1}{2}$不是整数。此矛盾说明不存在$\{R;\ +\}$到$\{Z;\ +\}$的同构映射。

第二章　群习题解答

§1

1　证　显然“$\circ$”是G的一个代数运算。

（1）$\forall a,b,c\in G$,

$$(a\circ b)\circ c=(a+b-3)\circ c=(a+b-3)+c-3$$
$$=a+(b+c-3)-3=a\circ(b+c-3)$$
$$=a\circ(b\circ c)$$

故满足结合律；

（2）易知3是$\{G;\ \circ\}$的恒等元；

（3）$\forall a\in G$，直接验算知$6-a$是a在$\{G;\circ\}$中的逆元。

故$\{G;\ \circ\}$是一个群。

2　证　因$a\neq 0$，$c\neq 0$，故$ac\neq 0$，且ac，$ad+b$均为实数，法则

$$(a,b)\cdot(c,d)=(ac,ad+b)$$

显然是G的代数运算。

（1）$\forall (a,b),(c,d),(e,f)\in G$,

$$(a,b)[(c,d)\cdot(e,f)]=(a,b)(ce,cf+d)$$
$$=(a(ce),a(cf+d)+b)=(ace,acf+ad+b)$$
$$[(a,b)\cdot(c,d)]\cdot(e,f)=(ac,ad+b)\cdot(e,f)$$
$$=((ac)e,(ac)f+ad+b)=(ace,acf+ad+b)$$

故　$(a,b)[c,d)\cdot(e,f)]=[(a,b)\cdot(c,d)]\cdot(e,f)$

结合律成立；

（2）显然$(1,0)$为G的左恒等元；

（3） $\forall (a,b)\in G$ 有$\left(\frac{1}{a},-\frac{b}{a}\right)\in G$为其左逆元．故$\{G;\cdot\}$是一个群．

3 证 $\forall (a_1,a_2),(b_1,b_2)\in G\times G$，因$\{G;\ \cdot\}$是代数体系，故$a_1\cdot b_1, a_2\cdot b_2\in G$，所以

$$(a_1,a_2)\circ(b_1,b_2)=(a_1\cdot b_1,a_2\cdot b_2)\in G\times G$$

故$\{G\times G;\ \circ\}$也是一个代数体系．

（1） $\forall (a_1,a_2),(b_1,b_2),(c_1,c_2)\in G\times G$．因$\{G;\ \cdot\}$是群，G的乘法满足结合律，于是有

$$((a_1,a_2)\circ(b_1,b_2))\circ(c_1,c_2)=(a_1b_1,a_2b_2)\circ(c_1,c_2)$$
$$=((a_1b_1)c_1,(a_2b_2)c_2)=(a_1(b_1c_1),a_2(b_2c_2))$$
$$=(a_1,a_2)\circ(b_1c_1,b_2c_2)=(a_1,a_2)\circ((b_1,b_2)\circ(c_1,c_2))$$

故“$\circ$”满足结合律；

（2） 设e是$\{G;\ \cdot\}$的恒等元，易知$(e,e)\in G\times G$是$\{G\times G;\ \circ\}$的恒等元；

（3） $\forall (a,b)\in G\times G, a,b\in G$，$a$，$b$有逆元为$a^{-1},b^{-1}\in G$，$(a^{-1},b^{-1})\in G\times G$，易知$(a^{-1},b^{-1})$是$(a,b)$的逆元．故$\{G\times G;\ \circ\}$是群．

4 必要性显然，充分性的证明完全仿照本章§1定理1的证明即可．

5 证 因G是群，$s\in G$，$\forall a$，$b\in G$，$a\circ b=asb\in G$，故“$\circ$”是G的一个代数运算．

（1） $\forall a,b,c\in G$，

$$(a\circ b)\circ c=(asb)\circ c=(asb)sc=as(bsc)$$
$$=a\circ(bsc)=a\circ(b\circ c)$$

故“$\circ$”满足结合律；

（2） 因$s\in G$，故$s^{-1}\in G$，$\forall a\in G$，有

$$a\circ s^{-1}=ass^{-1}=ae=a$$

故s^{-1}为$\{G;\ \circ\}$的右恒等元；

（3） $\forall a\in G$，有$a'=s^{-1}a^{-1}s^{-1}\in G$，使

$$a\circ a' = as(s^{-1}a^{-1}s^{-1}) = s^{-1}$$

故a'为 a 关于"∘"运算的右逆元，从而$\{G; \circ\}$是一个群。

6 **证** 必要性显然，只证充分性。

若 $(ab)^2 = a^2b^2$，即$ab\ ab = aa\ bb$

由消去律成立，左边消去 a，右边消去 b，即得

$$ab = ba, \forall a,b \in G$$

故G为交换半群。

7 **证** $\forall a,b\in G$，由题设有 $a^2 = e$，$b^2 = e$，即 $a = a^{-1}$，$b = b^{-1}$，又$ab\in G$，则有

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

因此，G是交换群。

8 **证** $\forall a\in G$，或者$a^2 = e$或者$a^2 \neq e$，二者必居其一。设

$$T = \{a\in G \mid a^2 = e\}, \quad S = \{a\in G \mid a^2 \neq e\}$$

显然$G = T\cup S$，且$T\cap S = \phi$，$\forall a\in S$，由$a^2\neq e$，知 $a\neq a^{-1}$，而$(a^{-1})^2 = (a^2)^{-1}\neq e$，故$a^{-1}\in S$，又$a\neq b$，则 $a^{-1}\neq b^{-1}$，故S中元素a，a^{-1}必成对出现，所以S的元素个数必为偶数。从而T中元素个数也必为偶数。由于$e^2 = e$，故$e\in T$，由T的元素个数为偶数知，至少有一个元素$a\neq e$在T中，即 $a^2 = e$，且此种元素个数必为奇数。

9 **证** 因G是群，$a,b\in G$，有$a^{-1},b^{-1}\in G$，令$x = a^{-1}bca^{-1}b^{-1}$，直接验证可知$a^{-1}bca^{-1}b^{-1}$是方程

$$xaxba = xbc$$

在G中的一个解。

若x_0是方程在G中的任一解，即

$$x_0ax_0ba = x_0bc$$

由消去律得

$$ax_0ba = bc$$

从而$x_0 = a^{-1}bca^{-1}b^{-1}$，故所给方程在G中有且仅有一个解。

10 **证** 因G为非交换群，故由第7题的结论知，G中必存在 $a^2\neq e$ 的元 a，即 $a\neq a^{-1}$，且 $a\neq e$，令 $b = a^{-1}\neq e$，那么

$ab=ba$。

§2

1　证　显然$e\in C(S)$，故$C(S)$非空。

（1）$\forall a,b\in C(S),\forall s\in S$，则有$as=sa$，$bs=sb$。于是

$$(ab)s=a(bs)=a(sb)=(as)b=(sa)b=s(ab)$$

故$ab\in C(S)$。

（2）$\forall a\in C(S)$，$\forall s\in S$，由$as=sa$，将此式两端各乘以a^{-1}，得$sa^{-1}=a^{-1}s$，从而$a^{-1}\in C(S)$。故$C(S)$为群G的子群。

2　证　因$eSe^{-1}=S,e\in N(S)$，故$N(S)$非空。$\forall b\in N(S)$，有$bSb^{-1}=S$，两边左乘b^{-1}，右乘b，$S=b^{-1}Sb$故$b^{-1}\in N(S)$。$\forall a,b\in N(S)$，则有

$$(ab^{-1})S(ab^{-1})^{-1}=ab^{-1}Sba^{-1}=a(b^{-1}Sb)a^{-1}=aSa^{-1}=S$$

即$ab^{-1}\in N(S)$，因此$N(S)$是G的子群。

因为S的中心化子

$$C(S)=\{x|x\in G,\forall s\in S,xsx^{-1}=s\}$$

故$C(S)\subseteq N(S)$。但$N(S)$中元未必属于$C(S)$。

3　证　先证$G^{(m)}$是G的子群．因G是交换群，$\forall a^m,b^m\in G^{(m)}$，则有

$$a^m(b^m)^{-1}=a^m(b^{-1})^m=(ab^{-1})^m\in G^{(m)}$$

故$G^{(m)}$是G的子群。

再证$G_{(m)}$是G的子群。$\forall a,b\in G_{(m)}$，则有$a^m=e,b^m=e$，于是

$$(ab^{-1})^m=a^m(b^{-1})^m=a^m(b^m)^{-1}=e\cdot e^{-1}=e$$

故$ab^{-1}\in G_{(m)}$，因此$G_{(m)}$是G的子群。

4　证　（1）任取x，$y\in H$，则存在自然数m,n，使$x^n=1$，$y^m=1$，令k是m，n的最小公倍数，即$k=[m,n]$，则$(xy)^k=1$，故H关于复数乘法封闭。

（2）若$x\in H$，则存在自然数n，使$x^n=1$，则$(x^{-1})^n=(x^n)^{-1}=1$，故，$x^{-1}\in H$．H是G的子群。

5　**证**　这四个矩阵是本章§1例3中的一般线性群$GL_2(R)$的有限子集，由判别条件3知这四个矩阵作成群，只需验证运算封闭即可。

列出乘法表

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

由表知运算封闭。故这四个矩阵作成群。

6　列出乘法表

	(1)	(12)(34)	(13)(24)	(14)(23)
(1)	(1)	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	(1)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	(1)	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	(1)

可知运算封闭．由判别条件3知B_4为S_3的子群．

7　**证**　$\forall ah_1a^{-1}, ah_2a^{-1}\in aHa^{-1}$，其中$h_1,h_2\in H$，则$ah_1a^{-1}\cdot ah_2a^{-1}=ah_1h_2a^{-1}=aha^{-1}\in aHa^{-1}$。又　$(aha^{-1})^{-1}=ah^{-1}a^{-1}\in aHa^{-1}$，故$aHa^{-1}$是G的子群。令

$$\varphi:\quad h\longmapsto aha^{-1}$$

显然φ是H到aHa^{-1}的双射，故H与aHa^{-1}为同阶子群。

8　**证**　$\forall a,b\in H$，存在i，j，使$a\in H_i$，$b\in H_j$，设i，j

中较大者为 j，则 $H_i \subseteq H_j$。于是 $a,b \in H_j$。因 H_j 为子群，故 $ab \in H_j$，于是 $ab \in H$。即 H 对G的乘法封闭。

又 $\forall a \in H$，$a \in H_i$，因 H_i 为子群，$a^{-1} \in H_i$，故 $a^{-1} \in H$。所以 H 是G的子群。

9 **解** S 生成的子群应包含下列元素：

$(12)^2 = (1)$，$(123)^2 = (132)$，$(12)(123) = (23)$，

$(12)(132) = (13)$

故 $(S) = S_3$。

一个群的两个不同的子集可能生成相同的子群。如取 S_3 的两个子集 $S_1 = \{(123)\}$，$S_2 = \{(132)\}$，$S_1 \neq S_2$，但 $(S_1) = (S_2) = \{(1),(123),(132)\}$。

10 **解** 由 a,b 生成的子群，运算必须封闭。其中必含有下列元素：

$$a \cdot a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = c$$

$$a^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = d$$

$$aa^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

$$ab = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = f$$

$$ba = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = g$$

$$af = a \cdot ab = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = h$$

$b^{-1} = b$，$ab^{-1}g = c$，……

乘法表为

$\cdot$	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	c	f	d	e	h	b	g
b	b	g	e	h	f	d	a	c
c	c	d	h	e	a	g	f	b
d	d	e	g	a	c	b	h	f
f	f	b	a	g	h	e	c	d
g	g	h	d	f	b	c	e	a
h	h	f	c	b	g	a	d	e

从上表可以看出

（1） $H=\{e,a,b,c,d,f,g,h\}$关于矩阵乘法封闭；

（2） e,b,c,f,g,h的逆元为自身．a,d互为逆元．

故H是由$S=\{a,b\}$生成的$GL_2(R)$的子群．其阶为 8 ．

11 **证** 必要性．设G的子集S是G的一组生成元．若存在G的真子群H，使得$S\subseteq H\subset G$．因H是一个群，而$S\subseteq H$，故S的元的幂和乘积必属于H．然而S是G的生成元集合，则G中任一元a皆可表为S的元的幂或乘积，即G中任一元$a\in H$．这与H是G的真子群矛盾．

充分性．设G中不存在包含S的真子群．令S生成的子群$(S)=K$，则$K\subseteq G$．但由假设G不含包含S的真子群，从而$K=G$，即$(S)=G$．这说明S是G的一组生成元．

12 **证** 设A，B是G的任意两个真子群，则存在$a,b\in G$，使$a\overline{\in} A$，$b\overline{\in} B$．

下面分三种情形讨论

（1）若$a\overline{\in} B$时，有$a\overline{\in} A\cup B$，故$G\neq A\cup B$；

（2）若$b \in A$时，有$b \bar{\in} A \cup B$，故$G \neq A \cup B$；

（3）若$a \in B$且$b \in A$时，则$ab \bar{\in} A \cup B$。

事实上，若$ab \in B$，由$a \in B$，B为子群，则$a^{-1} \in B$，从而有$a^{-1}ab = b \in B$，这与$b \bar{\in} B$矛盾。故$ab \bar{\in} B$同理可证$ab \bar{\in} A$，因此$ab \bar{\in} A \cup B$，所以$G \neq A \cup B$。

§3

1 **证** 令φ：$n \longmapsto 2n$，$\forall n \in \mathbf{Z}$。易证此映射φ是$\{\mathbf{Z};+\}$到偶数加群的同构映射。

2 **证** 令$\varphi: A \longmapsto |A|$，$\forall A \in GL_n(\mathbf{R})$，显然$\varphi$是$GL_n(\mathbf{R})$到$\dot{\mathbf{R}}$的满射。又$\varphi(AB) = |A \cdot B| = |A| \cdot |B| = \varphi(A) \cdot \varphi(B)$。故$\varphi$是$G$到$G'$的满同态，所以$G \sim G'$。

3 **解** 显然φ是G到G'的满射。又

$$\varphi(\theta_1 + \theta_2) = e^{i(\theta_1 + \theta_2)} = e^{i\theta_1} \cdot e^{i\theta_2} = \varphi(\theta_1) \cdot \varphi(\theta_2)$$

故φ保持运算。

在G'中由于$e^{i\theta} = e^{i(\theta + 2k\pi)}$，$k = 0, 1, 2, \cdots$。而在$G$中$\theta \neq \theta + 2k\pi$　$(k \neq 0)$，但$\varphi(\theta) = \varphi(\theta + 2k\pi)$。故$\varphi$不是单射。所以$\varphi$不是$G$到$G'$的同构映射，而只是满同态。故在$\varphi$之下$G$与$G'$不同构，但$G \sim G'$。由$G$是群知$G'$也是群。

4 **证** 令φ：$1 \longmapsto \sigma_0$，$i \longmapsto \sigma_{\frac{\pi}{2}}$，$-1 \longmapsto \sigma_\pi$，$-i \longmapsto \sigma_{\frac{3\pi}{2}}$。显然$\varphi$是$G$到$G'$的同构映射。故$G \cong G'$。由$G$是群知$G'$也是群。

5 **证** $\forall a \in C(G)$，$\varphi(a) = a' \in G'$。下面证明：$\varphi(a) = a' \in C(G')$。$\forall x' \in G'$。由$\varphi$为满射，故有$x \in G$，使$\varphi(x) = x'$。因$a \in C(G)$，故有$ax = xa$。由$\varphi$是$G$到$G'$的同态映射，于是有，$a'x' = \varphi(a)\varphi(x) = \varphi(ax) = \varphi(xa) = \varphi(x) \cdot \varphi(a) = x'a'$。故$a' \in C(G')$

6 **证** 若G为可换群，$\forall a \in G$，有$a^{-1} \in G$，使$\varphi(a^{-1}) = (a^{-1})^{-1} = a$。故$\varphi$为满射。显然，若$a \neq b$，则$a^{-1} \neq b^{-1}$，即$\varphi(a) \neq$

$\varphi(b)$，故 φ 为单射。又

$$\varphi(a\cdot b)=(ab)^{-1}=b^{-1}a^{-1}=a^{-1}b^{-1}=\varphi(a)\cdot\varphi(b)$$

故 φ 是G的自同构映射。

反之，若 φ 是 G 的自同构映射。$\forall a,b\in G$，有 $a^{-1},b^{-1}\in G$，使 $\varphi(a^{-1})=a$，$\varphi(b^{-1})=b$。$\varphi(a^{-1}b^{-1})=\varphi(a^{-1})\ \varphi(b^{-1})=ab$；又 $\varphi(a^{-1}b^{-1})=\varphi((ba)^{-1})=ba$。故 $ab=ba$。因此 G 是可换群。

7　证（1）若 H 是G的子群，则 $\varphi(H)$ 非空。$\forall a',b'\in\varphi(H)$，存在 $a,b\subset H$，使得 $\varphi(a)=a',\varphi(b)=b'$。于是 $a'b'^{-1}=\varphi(a)(\varphi(b))^{-1}=\varphi(a)\varphi(b^{-1})=\varphi(ab^{-1})$。因 $ab^{-1}\in H$，所以 $a'b'^{-1}\in\varphi(H)$。故 $\varphi(H)$ 是 G' 的子群。

（2）若 H' 是 G' 的子群，则 $\varphi^{-1}(H')$ 非空。$\forall a,b\in\varphi^{-1}(H')$，则 $\varphi(a)$，$\varphi(b)\in H'$。因 H' 是 G' 的子群，$\varphi(b)^{-1}=\varphi(b^{-1})\in H'$。于是 $\varphi(ab^{-1})=\varphi(a)\varphi(b^{-1})\in H'$。即 $ab^{-1}\in\varphi^{-1}(H')$。故 $\varphi^{-1}(H')$ 是 G' 的子群。

§4

1　证　设 a 的阶为 n，a^{-1} 的阶为 m。由 $a^n=e\Longrightarrow(a^{-1})^n=(a^n)^{-1}=e$。故 a^{-1} 的阶 $m\leqslant n$；反之，由 $(a^{-1})^m=e\Longrightarrow a^m=((a^{-1})^{-1})^m=((a^{-1})^m)^{-1}=e^{-1}=e$。故 $n\leqslant m$。从而 $n=m$。即 a 与 a^{-1} 同阶。

设 ab 的阶为 n，ba 的阶为 m。由 $(ab)^n=e\Longrightarrow(ba)^n=(a^{-1}aba)^n=a^{-1}(ab)^na=a^{-1}ea=e$，故 $m\leqslant n$，同理可证 $n\leqslant m$。故 ab 与 ba 的阶相同。

2　证　若 $n\backslash m$，$m=nq$，显然 $a^m=(a^n)^q=e$；反之，令 $m=nq+r(0\leqslant r<n)$，则 $a^m=a^{nq+r}=(a^n)^q\cdot a^r=a^r=e$。由 a 的阶为 n，必有 $r=0$，故 $n\backslash m$。

3　证　$\forall x\in G$，易证 $x^{-1}ax$ 与 a 同阶，故由题设有 $x^{-1}ax=a$，于是 $xa=ax$。

4　证　若 a 的阶大于2，则 $a\neq a^{-1}$，否则将有 $a^2=e$ 与 a 的阶大于2矛盾。由第1题知 a 与 a^{-1} 同阶。因此，阶大于2

的元素必成对出现．故在有限群中阶大于 2 的元素个数必是偶数．

5　$\{Z_4;\ +\}$中$\overline{0}$的阶为 1，$\overline{1}$和$\overline{3}$的阶为 4，$\overline{2}$的阶为 2．$\{S_3;\ \cdot\}$中（1）的阶为 1，(12)，(13)，(23) 的阶为 2，(123)，(132)的阶为 3．

6　**证**　设$G=(a)$为循环群．$\forall x,y\in G$，则 $x=a^m$，$y=a^n$，$xy=a^m\cdot a^n=a^{m+n}=a^{n+m}=a^n\cdot a^m=y\cdot x$．故循环群必为交换群．

7　**证**　设ab的阶为 k，去证 $k=mn$．由于 $ab=ba$，所以 $(ab)^{mn}=a^{mn}\cdot b^{mn}=(a^m)^n\cdot(b^n)^m=e^n\cdot e^m=e$．故$k\backslash mn$．

又　$(ab)^{km}=a^{km}\cdot b^{km}=(a^m)^k\cdot b^{km}=b^{km}$，而　$(ab)^{km}=e$，故 $b^{km}=e$．从而$n\backslash km$．但$(m,n)=1$，因此$n\backslash k$，同理可证$m\backslash k$．再利用$(m,n)=1$，有$mn\backslash k$．所以$k=mn$．即ab的阶为mn．

若$ab\neq ba$，此结论未必成立．例如，在S_3中，取$a=(12)$，$b=(132)$，已知 a 的阶为 2，b 的阶为 3，且$(2,3)=1$，但$ab\neq ba$，$ab=(13)$的阶为$2\neq 2\times 3$

8　**证**　首先确定由a,b生成的群的元素的形状．因 $ab=ba$，$a^2=e$，即$a=a^{-1}$，$a^m=a^{-m}$，$b^3=e$，$b^{-1}=b^2$．故由 a,b 生成的群 $G=(a,b)$的元素一般形状为：

$$a^mb^n,\ m=0,\ 1;\ n=0,1,2$$

共有六种取法．即$G=(a,b)$为6阶群．又知 a 的阶为 2，b 的阶为 3，$(2,3)=1$，故由上题知ab的阶为 6，从而$G=(a,b)=(ab)$为 6 阶循环群．其 6 个元素表法如下

$$a^0b^0=e=(ab)^0,\ a^0b=b=(ab)^4,\ a^0b^2=b^2=(ab)^2,$$
$$ab^0=a=(ab)^3, ab=(ab), ab^2=(ab)^5$$

9　**证**　方法一：如果a^r是无限循环群$G=(a)$的一个生成元，则(a)中每一元皆为a^r的方幂，特别地，a 也可表为 a^r的方幂，即$a=(a^r)^m$．因 a 为无限阶元素，上式成立当且仅当$rm=1$，故$r=\pm 1$．故无限阶循环群只有两个生成元 a 和a^{-1}．

方法二：因 $G\cong Z$ 。只须证 Z 有且只有两个生成元即可。证法同上。

10　证　设 a^r 的阶为 m，往证 $m=\frac{n}{d}$・因 $(r, n)=d$，故 $r=dr_1, n=dn_1$，且 $(r_1,n_1)=1$。

$$(a^r)^{\frac{n}{d}}=(a^r)^{n_1}=a^{dr_1n_1}=(a^n)^{r_1}=e^{r_1}=e$$

由第 2 题知 $m\backslash\frac{n}{d}$ 。

又 $(a^r)^m=a^{rm}=e$，因 a 的阶为 n，故 $n\backslash rm\Longrightarrow dn_1\backslash dr_1m$ $\Longrightarrow n_1\backslash r_1m$，但 $(r_1,n_1)=1\Longrightarrow n_1\backslash m$，即 $\frac{n}{d}\backslash m$.故 $m=\frac{n}{d}$。即 a^r 的阶为 $\frac{n}{d}$。

11　证　若 $(r,n)=1$，由上题知 a^r 的阶为 n，故 $(a^r)=G$，a^r 也是 G 的生成元。反之，若 a^r 为 G 的生成元，则 $a=(a^r)^m=a^{rm}$，因 a 的阶为 n，上式成立当且仅当 $n\backslash rm-1$，即 $rm-1=nq$ 或 $rm-nq=1$，所以 $(r, n)=1$。

12　解　由上题知 Z_{12} 的生成元共有 4 个为：$\overline{1}$，$\overline{5}$，$\overline{7}$，$\overline{11}$。子群共有 6 个为

$$H_1=\{\overline{0}\}, H_2=\{\overline{0}, \overline{6}\}=(\overline{6})$$

$$H_3=\{\overline{0}, \overline{4}, \overline{8}\}=(\overline{4})$$

$$H_4=\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}=(\overline{3})$$

$$H_5=\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}=(\overline{2}), H_6=Z_{12}$$

13　证　分两种情形

（1）若 $G'=(a')$ 是无限阶循环群，$G=(a)$。令

$$\varphi:\ a^m\longmapsto a'^m\quad \forall m\in Z$$

显然 φ 是 G 到 G' 的满射，且

$$\varphi(a^m\cdot a^n)=\varphi(a^{m+n})=a'^{m+n}=a'^m\cdot a'^n=\varphi(a^m)\varphi(a^n)$$

故$G\sim G'$.

（2）若$G'=(a')$为n阶循环群，即a'的阶为n. $\forall\ a^{m_1}\in G$，令

φ: $a^{m_1}\longmapsto a'^{r_1}$ 当且仅当$m_1=nq_1+r_1$，$0\leqslant r_1<n$. 易知φ是G到G'的满射. 又

$$a^{m_2}\longmapsto a'^{r_2},\quad m_2=nq_2+r_2, 0\leqslant r_2<n$$

设 $r_1+r_2=nq+r$，$0\leqslant r<n$，则

$$m_1+m_2=n(q_1+q_2)+r_1+r_2=n(q_1+q_2+q)+r$$

于是

$$\varphi(a^{m_1}\cdot a^{m_2})=\varphi(a^{m_1+m_2})=a'^{r}=a'^{r}\cdot a'^{nq}=a'^{nq+r}$$
$$=a'^{r_1+r_2}=a'^{r_1}\cdot a'^{r_2}=\varphi(a^{m_1})\cdot\varphi(a^{m_2})$$

故$G\sim G'$.

另法：由循环群的构造定理知，$G\overset{\psi}{\cong}Z$，$Z_n\overset{f}{\cong}G'$. 只要证明$Z\overset{\varphi}{\sim}Z_n$，即有$G\overset{\psi}{\cong}Z\overset{\varphi}{\sim}Z_n\overset{f}{\cong}G'$从而$G\sim G'$. 易证$\varphi: m\longmapsto\overline{r}$，$m=nq+r$，$0\leqslant r<n$是$Z$到$Z_n$的同态映射. 于是$\sigma=f\varphi\psi$是$G$到$G'$的同态映射.

14 证 若$G\overset{\varphi}{\cong}G'$，$\forall a\in G$.

φ: $a\longmapsto a'$

则有$a^n=e\Longleftrightarrow a'^n=e'$. 故$a$与$a'$有相同的阶.

若$G\overset{\varphi}{\sim}G'$，则可由$a^n=e$推出$a'^n=e'$. 反之未必成立. 这说明$a'$的阶是$a$的阶的约数，两者不一定相同.

例如，$G=\{1,i,-1,-i\}$，$G'=\{1,-1\}$. 由第一章§5习题2知，在映射φ: $\pm1\longmapsto1$，$\pm i\longmapsto-1$之下$G\sim G'$. G中-1的阶为2，但-1的象为1，它的阶不等于2而是1. 又$\pm i$的阶均是4，而它们的象-1的阶为2.

§5

1　证　设所给变换的集合为$T(R)$。首先证明$T(R)$中任一变换$\varphi_{a,b}$皆为R的双变换。$\forall x\in R$，有 $y=\frac{1}{a}x-\frac{b}{a}\in R$，

使$\varphi_{a,b}(y)=a\left(\frac{1}{a}x-\frac{b}{a}\right)+b==x$，故 $\varphi_{a,b}$为R的满变换。又

若 $x\neq y$，显然$ax+b\neq ay+b$，$\varphi_{a,b}$ 为R的单变换。从而 $\varphi_{a,b}$为R的双变换。

$\forall \varphi_{a,b}$，$\varphi_{c,d}\in T(R)$，则$\varphi_{a,b}\cdot\varphi_{c,d}(x)=\varphi_{a,b}(\varphi_{c,d}(x))=\varphi_{a,b}(cx+d)=a(cx+d)+b=acx+(ad+b)$。由$a\neq0$，$c\neq0$，有$ac\neq0$，故$T(R)$对于变换乘法封闭。

（1）变换乘法显然满足结合律；

（2）易见I_R：$x\longmapsto x$是$T(R)$的恒等元；

（3）$\forall\varphi_{a,b}\in T(R)$，若有$\varphi_{c,d}\in T(R)$，使 $\varphi_{c,d}\cdot\varphi_{a,b}=I_R$，则由$\varphi_{c,d}\cdot\varphi_{a,b}(x)=\varphi_{c,d}(ax+b)=cax+cb+d=I_R(x)=x$，$\forall x\in R$，得 $ca=1$，$cb+d=0$，由此知 $c=\frac{1}{a}$，$d=-\frac{b}{a}$，

故$T(R)$中每一元$\varphi_{a,b}$皆有逆元为 $\varphi_{\frac{1}{a},-\frac{b}{b}}$。

所以$T(R)$作成一个变换群。

取$\varphi_{1,1}$：$x\longmapsto x+1$，$\varphi_{2,0}$：$x\longmapsto 2x$，则有

$$\varphi_{1,1}\cdot\varphi_{2,0}(x)=2x+1，\quad \varphi_{2,0}\cdot\varphi_{1,1}(x)=2(x+1)$$

显然$\varphi_{1,1}\cdot\varphi_{2,0}\neq\varphi_{2,0}\cdot\varphi_{1,1}$，因此$T(R)$不是交换群。

2　证　设ε是变换群G的恒等元。$\forall\tau\in G$，τ 是集合A的双变换，因此$\forall a\in A$，有元$b\in A$，使得$\tau(b)=a$。于是

$$\varepsilon(a)=\varepsilon(\tau(b))=\varepsilon\tau(b)=\tau(b)=a$$

故 ε 为恒等变换，即$\varepsilon=I_A$。

3　解　$\forall\varphi_a$，$\varphi_b\in T$，其中

$\varphi_a:(x,y)\longmapsto(x+a,0)$，$\varphi_b:(x,y)\longmapsto(x+b,0)$则$\varphi_a\cdot\varphi_b$ $(x,y)=\varphi_a(\varphi_b(x,y))=\varphi_a((x+b,0))=(x+b+a,0)$故$\varphi_a\cdot\varphi_b$ $=\varphi_{a+b}\in T$.T对变换乘法封闭.

（1）结合律显然成立；

（2）$\varphi_0:(x,y)\longmapsto(x,0)$显然是$T$的恒等元；

（3）$\forall\varphi_a\in T$,有$\varphi_{-a}\in T$，使$\varphi_{-a}\cdot\varphi_a=\varphi_0$,即$\varphi_a{}^{-1}=\varphi_{-a}$.
故T关于变换乘法作成群.

由于T的恒等元φ_0不是恒等变换，由上题结论知T不是变换群．显然平面π上的点$(x,1)$在φ_a之下没有原象，φ_a不是双变换.

4　解　令 $e=\begin{pmatrix}1&0\\0&1\end{pmatrix}$，　$a=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$，　$b=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$，
$c=\begin{pmatrix}-1&0\\0&1\end{pmatrix}$.利用$G$的元,按照§5定理2的方法仿照§5例3得

$$\tau_e: x\longmapsto ex,\quad \forall x\in G$$
$$\tau_a: x\longmapsto ax,\quad \forall x\in G$$
$$\tau_b: x\longmapsto bx,\quad \forall x\in G$$
$$\tau_c: x\longmapsto cx,\quad \forall x\in G$$

故

$$\tau_e=\begin{pmatrix}e&a&b&c\\e&a&b&c\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=(1)$$

$$\tau_a=\begin{pmatrix}e&a&b&c\\a&e&c&b\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(12)(34)$$

$$\tau_b=\begin{pmatrix}e&a&b&c\\b&c&e&a\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(13)(24)$$

$$\tau_c=\begin{pmatrix}e&a&b&c\\c&b&a&e\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(14)(23)$$

$\overline{G}=\{\tau_e,\tau_a,\tau_b,\tau_c\}=\{(1),(12)(34),(13)(24),(14)(23)\}$ $=B_4$　即为与G同构的置换群.

5　证　令$\sigma:\varphi_{a,b}\longmapsto(a,b)$：易证$\sigma$是第1题中的变换

群$T(R)$到§1习题2中的群G的同构映射。

§6

1　解　显然$H=eH$是G的一个左陪集。若H的左陪集aH也是G的一个子群，则$e\in aH$，$a^{-1}e\in a^{-1}(aH)=H$。故$a\in H$。从而$aH=H$。故H的所有左陪集中只有H是G的子群。

2　解　两个实数a,b属于H的同一陪集当且仅当$a-b\in H$，故G关于H的每一陪集都是由相差为整数的实数组成的。若把每一实数看成数轴上的一个点，则每一陪集是这样的点的集合；这些点都以相似位置分布在以整数为端点的各个单位区间内。如…，-1.9，-0.9，0.1，1.1，2.1，…在同一陪集中，而0.1和0.2在不同陪集中。各陪集的代表可取做左闭右开区间$[0,1)$的所有实数。$[0,1)$中任意两个实数属于H的不同陪集，故H在G中的指数为无限。

3　证　按照(1)$\Longrightarrow$(2)$\Longrightarrow$(3)$\Longrightarrow$(4)$\Longrightarrow$(5)$\Longrightarrow$(6)$\Longrightarrow$(1)的顺序证明之。

(1)$\Longrightarrow$(2)　因H是子群，由$b^{-1}a\in H$得$(b^{-1}a)^{-1}=a^{-1}b\in H$。

(2)$\Longrightarrow$(3)　由$a^{-1}b\in H$，有$h'\in H$使$a^{-1}b=h'$，所以$b=ah'\in aH$。

(3)$\Longrightarrow$(4)　由$b\in aH$，有$h''\in H$使$b=ah''$，所以$a=bh''^{-1}\in bH$。

(4)$\Longrightarrow$(5)　由$a\in bH$有$a=bh$，从而$aH\subseteq bH$，而$b=ah^{-1}$，故有$bH\subseteq aH$，于是得到$aH=bH$。

(5)$\Longrightarrow$(6)　由$aH=bH$，至少有a，$b\in aH\cap bH$，故$aH\cap bH\neq\phi$。

(6)$\Longrightarrow$(1)　若$aH\cap bH\neq\phi$，设$x\in aH\cap bH$，则有$x=ah_1=bh_2$，$h_1,h_2\in H$。从而有$b^{-1}a=h_2h_1^{-1}\in H$。

4　证　因素数$p>1$，在G中有$a\neq e$，(a)是G的子群，

其阶为m，由拉格朗日定理知$m\backslash p$． 易见$m\neq 1$，否则$a=e$。故$m=p$。所以$G=(a)$。

5 证 $\forall a\in G$:(a)为G的子群，其阶为m，即a的阶为m。由拉格朗日定理知$m\backslash n$，即$n=mq$，故$a^n=(a^m)^q=e$。

6 证 只要证$H\cap K$的阶为1即可。

7 证 设Q_1和Q_2分别是H_1与H_2的商集，其元素个数为m和n。设Q为$H_1\cap H_2$的商集．去证：$\forall a(H_1\cap H_2)\in Q$，必有$a(H_1\cap H_2)=aH_1\cap aH_2$。

事实上，$\forall ah\in a(H_1\cap H_2)$，$h\in H_1\cap H_2$:$h\in H_1$，$h\in H_2$，有$ah\in aH_1$,$ah\in aH_2$．故$ah\in aH_1\cap aH_2$,$a(H_1\cap H_2)\subseteq aH_1\cap aH_2$。反之，$\forall x\in aH_1\cap aH_2$有$x\in aH_1$,$x\in aH_2$。于是有$h_1\in H_1$，$h_2\in H_2$，使$x=ah_1=ah_2$。由消去律有$h_1=h_2$，故$h_1\in H_1\cap H_2$，于是$x\in a(H_1\cap H_2)$，$aH_1\cap aH_2\subseteq a(H_1\cap H_2)$， 因此$a(H_1\cap H_2)=aH_1\cap aH_2$。此式表明$H_1\cap H_2$的任一陪集（$Q$中的任一元素）都可表为$H_1$的一个陪集($Q_1$中的元素)与$H_2$的一个陪集($Q_2$中的元素)的交，而这种形式的交最多有$m\cdot n$个，故$Q$的元素个数是有限的。

8 证 已知S_3为非交换群．显然一阶群$\{e\}$为交换群．又知阶数为2，3，5（素数）阶的群都是循环群，故为交换群。剩下只须证明4阶群G是交换群．

如果G中有4阶元素，则G是循环群，从而是交换群．如果G中无4阶元素，则元素的阶必为1或2，所以$\forall x\in G$总有$x^2=e$。由§1习题7可知G是交换群．故S_3是阶数最小的非交换群。

9 证 只要证明6阶群中必有阶为3的元即可。G中非恒等元的元的阶不能都是2，否则，G为交换群，且$H=\{e,a,b,ab\}$为G的4阶子群，但$4\nmid 6$，与拉格朗日定理矛盾．故G中必有阶不是2的元g。由§6定理3知，g的阶只能是3或6。若g的阶为3，则$K=(g)$即为G的3阶子群．若g的阶为6，则$G=(g)$为循环群，此时，$K=(g^2)$即为3阶子群。

10 证 在G中任取$a \neq e$，由§6定理3知a的阶是$p^n (n \leqslant m)$。显然$a^{p^{n-1}}$的阶为p。故$H = (a^{p^{n-1}})$是G的阶为p的子群。

11 证 根据§6定理3，4阶群G的元素的阶只能是1，2，4。下分两种情形

（1）若G中含有阶为4的元素a，则$G = (a)$为4阶循环群；

（2）若G中不含阶为4的元，则除恒等元e外，其余各元的阶均为2，G必为交换群（§1习题7）。设$G = \{e, a, b, c\}$。可以断言，$ab \neq a$。如果$ab = a$，由消去律得$b = e$，这与G为4阶群矛盾。同理$ab \neq b$。又由于a, b的阶均为2，其逆元为自身，故$ab \neq e$，因此必有$ab = ba = c$。同样可证：$ac = ca = b$，$bc = cb = a$。又$a^2 = b^2 = c^2 = e$。于是G的乘法表为

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

而B_4的乘法表为

·	(1)	(12)(34)	(13)(24)	(14)(23)
(1)	(1)	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	(1)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	(1)	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	(1)

$$\varphi: e \longmapsto (1), \quad a \longmapsto (12)(34)$$

$$b \longmapsto (13)(24), \quad c \longmapsto (14)(23)$$

显然φ是G到B_4的双射．从上面两张乘法表完全重合可知φ是G到B_4的同构映射．故

$$G \cong B_4$$

§7

1　**证**　设H_1，H_2是群G的两个正规子群．已知$H_1 \cap H_2$是G的子群．$\forall g \in G, h \in H_1 \cap H_2$：有$h \in H_1, h \in H_2$，$ghg^{-1} \in H_1$，$ghg^{-1} \in H_2$．从而有$ghg^{-1} \in H_1 \cap H_2$，故$H_1 \cap H_2$是$G$的正规子群．

2　**证**　设$H = \{e, a\}$是G的二阶正规子群．显然$e \in C(G)$．$\forall g \in G$：由H为正规子群，有$gag^{-1} \in H$．若$gag^{-1} = e$，则$a = e$，这与$a \neq e$不合．故必有$gag^{-1} = a, ga = ag$，故$a \in C(G)$．得到$H \subseteq C(G)$．

3　由正规子群和正规化子的定义结论是明显的．

4　**证**　任取H的两个左陪集aH，bH．先证$aH \cdot bH = abH$．由题设$aH \cdot bH$是一个左陪集，设$aH \cdot bH = cH$．则$ab = ae \cdot be \in aH \cdot bH$，从而有$ab \in CH$．于是$abH = cH$，故$aH \cdot bH = abH$．

$\forall h \in H$，$a \in G$，有$ah \cdot a^{-1}h \in aHa^{-1}H = (aa^{-1})H = H$，所以$aha^{-1} \in H$．故$H$是$G$的正规子群．

5　**证**　由§2习题7知，$\forall a \in G, aHa^{-1}$也是$G$的$n$阶子群，再由题设有$aHa^{-1} = H$．故$H$为$G$的正规子群．

6　**证**　因A是正规子群，$\forall g \in G$，有$gA = Ag$，$\forall a \in A$，存在$a' \in A$，使$ga = a'g$．于是$\forall ab$，$a_1b_1 \in AB$，有

$$(ab)(a_1b_1) = a(ba_1)b_1 = a(a_1'b)b_1 = (aa_1')(bb_1) \in AB$$

又$(ab)^{-1} = b^{-1}a^{-1} = a''b^{-1} \in AB$（因为$a^{-1} \in A$）故$AB$是$G$的一个子群．

7　**证**　由上题知AB是G的子群，下面只证AB是G的正规子群．

$\forall g \in G$，$ab \in AB$，$a \in A$，$b \in B$.有

$$g(ab)g^{-1} = (gag^{-1})(gbg^{-1}) \in AB$$

故AB是G的正规子群。

8　证　由§2习题8知H为G的子群．$\forall a \in G, h \in H$，存在i，使$h \in H_i$，由H_i为G的正规子群，故$aha^{-1} \in H_i$，从而$aha^{-1} \in H$。故H为G的正规子群。

9　取$G = S_4$，$N = B_4 = \{(1),(12)(34),(13)(24),(14)(23)\}$，$K = \{(1),(13)(24)\}$。

已知$N = B_4$是G的子群．下证N是G的正规子群。

$$\forall a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix} \in S_3$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}(12)(34)\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}^{-1} = (i_1 i_2)(i_3 i_4) \in N$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}(13)(24)\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}^{-1} = (i_1 i_3)(i_2 i_4) \in N$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}(14)(23)\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}^{-1} = (i_1 i_4)(i_2 i_3) \in N$$

由此说明，$\forall a \in G, \forall n \in N, ana^{-1} \subset N$.故$N$为$G$的正规子群。

因为N为4阶交换群，故其子群K是N的正规子群．但K却不是G的正规子群．因为

$$(23)[(13)(24)](23)^{-1} = (12)(34) \in K$$

10　证　易证H是G的正规子群．若G/H是循环群，aH是G/H的生成元，则G中任意两元g_1，g_2必有$g_1 \in (aH)^{i_1} = a^{i_1}H$，$g_2 \in (aH)^{i_2} = a^{i_2}H$.于是$g_1 = a^{i_1}h_1, g_2 = a^{i_2}h_2, h_1$，$h_2 \in H$.注意到$H$中的元与$G$中元可交换，$a^{i_1}$与$a^{i_2}$可交换．于是

$$g_1 g_2 = a^{i_1}h_1 a^{i_2}h_2 = a^{i_2}h_2 a^{i_1}h_1 = g_2 g_1$$

故G是可换群。

11　证　（1）因$e = eee^{-1}e^{-1}$，故$e \in C$．（有限个换位子的乘积）·（有限个换位子的乘积）= 有限个换位子的乘积．故C对G的乘法封闭。

由于$(aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$仍是换位子，故有限个换位子

的乘积的逆元仍是有限个换位子的乘积。即若$c\in C$,则$c^{-1}\in C$。故C是G的子群（其实C即由所有换位子生成的子群）。

下证C是G的正规子群。$\forall c\in C, g\in G$,由$gcg^{-1}c^{-1}\in C$,有$gcg^{-1}\cdot c^{-1}c\in C$，即$gcg^{-1}\in C$。故$C$为$G$的正规子群。

（2）$\forall g_1C$，$g_2C\in G/C$。由

$$g_1Cg_2C\cdot g_1^{-1}C\cdot g_2^{-1}C=g_1g_2g_1^{-1}g_2^{-1}C=C$$

故

$$g_1C\cdot g_2C=g_2C\cdot g_1C$$

即G/C是交换群。（注意C是G/C的恒等元）

（3）设$aba^{-1}b^{-1}$为任意换位子，由G/N为可换群，故
$aN\cdot bN==bN\cdot aN$，即$aN\cdot bNa^{-1}N\cdot b^{-1}N=N$
$aba^{-1}b^{-1}N=N$
这就推出$aba^{-1}b^{-1}\in N$，从而$C\subseteq N$。

12 证 对n用数学归纳法。

当$n=2$时，命题显然成立。

假设对$m<n$时命题成立，去证当$m=n$时命题也成立。

取$a\in G$，$a\neq e$。设a的阶为k。则$k\backslash n$，如果$p\backslash k$，则$b=a^{\frac{k}{p}}$的阶为p，于是命题成立；如果$p\nmid k$,因G是交换群,故(a)是G的正规子群。$G/(a)=\overline{G}$为交换群，$\overline{G}$的阶数$m<n$，且$m\backslash n$。由于$mk=n=ps, p\backslash mk$,但$p\nmid k$，故必有$p\backslash m$。由归纳假设$\overline{G}$中存在阶为p的元$\overline{c}$，由$\overline{c}^p=\overline{c^p}=\overline{e}$（$\overline{e}$为$\overline{G}$的恒等元），可知$c^p\in(a)$,因$(a)$为$k$阶循环群，故$(c^p)^k=e$，即$(c^k)^p=e$，由$p$为素数，故$c^k$的阶或者是$p$或者是1，若$c^k=e$，有$\overline{c}^k=\overline{e}$即$\overline{c}^k=\overline{e}$，而$\overline{c}$的阶为$p$，故有$p\backslash k$,这与$p\nmid k$矛盾。此矛盾表明$c^k$的阶为$p$，即命题对任意$n$均成立。

13 证 充分性是明显的，只证必要性。设G的阶是一个合数，在G中取一个元素$a\neq e$，如果a的阶小于G的阶，那么，a生成的循环群就是G的一个非平凡子群，如果a的阶等于G的阶n，取n的一个真约数k，$1<k<n$，令$b=a^k$。

那么，b 就是 G 中一个阶小于 n 的非恒等元，(b) 就是 G 的一个非平凡子群。

§8

1　证　显然 φ 是 G 到自身的映射，$\forall a,b\in G$，因 G 是可换群，所以有

$$\varphi(ab)=(ab)^k=a^kb^k=\varphi(a)\varphi(b)$$

故 φ 是 G 的自同态映射。

$$\text{im}\varphi=\{a^k\mid a\in G\},\text{Ker}\varphi=\{x\in G\mid x^k=e\}$$

2　证　必要性。设 $\varphi(a)=\varphi(b)$，即 $\varphi(a)\varphi(b)^{-1}=\varphi(a)\varphi(b^{-1})=\varphi(ab^{-1})=e'$，故 $ab^{-1}\in N$，则 a,b 在 N 的同一陪集中。

充分性。若 a,b 在 N 的同一陪集中，即 $ab^{-1}\in N$，则 $\varphi(ab^{-1})=\varphi(a)\varphi(b^{-1})=\varphi(a)\varphi(b)^{-1}=e'$，故 $\varphi(a)=\varphi(b)$。即 a,b 在 G' 中有相同的象。

3　证　$\forall hk\in HK$，其中 $h\in H$，$k\in K$，

$\varphi(hk)=\varphi(h)\varphi(k)=\varphi(h)e'=\varphi(h)\in\varphi(H)$。故 $HK\subseteq\varphi^{-1}(\varphi(H))$（$e'$ 是 G' 的恒等元）。

$\forall x\in\varphi^{-1}(\varphi(H))$，则 $\varphi(x)\in\varphi(H)$。故存在 $h\in H$，使 $\varphi(x)=\varphi(h)$，于是 $\varphi(h^{-1}x)=\varphi(h^{-1})\varphi(x)=\varphi(h)^{-1}\varphi(x)=e'$。故 $h^{-1}x\in K$，即存在 $k\in K$，使 $h^{-1}x=k$，即 $x=hk\in HK$。故 $\varphi^{-1}(\varphi(H))\subseteq HK$。从而 $\varphi^{-1}(\varphi(H)=HK$

显然当 $H\supseteq K$ 时，有 $\varphi^{-1}(\varphi(H))=H$。

4　证　由题设条件 φ 是 G 到 G' 的满同态映射，故 φ 是 G 到 G' 的同构映射 $\Longleftrightarrow\varphi$ 为单射。

若 φ 为单射，即 $\varphi(a)=\varphi(b)$，必有 $a=b$，　$\forall x\in\varphi^{-1}(e')$，则 $\varphi(x)=\varphi(e)=e'$，故 $x=e$，即 $\varphi^{-1}(e')=\{e\}$。

反之，若 $\varphi^{-1}(e')=\{e\}$。$\forall a,b\in G$。若 $\varphi(a)=\varphi(b)$，则 $\varphi(a)\varphi(b)^{-1}=\varphi(ab^{-1})=e'$，故 $ab^{-1}\in\varphi^{-1}(e')=\{e\}$，即 $ab^{-1}=e$，于是 $a=b$。因此 φ 是单射。

5　证　（1）由§3习题7已知$\varphi(H_1)$是G_2的子群，只证$\varphi(H_1)$是G_2的正规子群.

$\forall g' \in G_2, h' \in \varphi(H_1)$，则存在$g \in G_1$，$h \in H_1$使得$\varphi(g) = g'$，$\varphi(h) = h'$，于是

$$g'h'g'^{-1} = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(ghg^{-1})$$

因H_1是G_1的正规子群，故$ghg^{-1} \in H_1$，从而$g'h'g'^{-1} = \varphi(ghg^{-1}) \in \varphi(H_1)$，故$\varphi(H_1)$是$G_2$的正规子群.

（2）$\forall g \in G_1$，$h \in \varphi^{-1}(H_2)$，则$\varphi(g), \varphi(g)^{-1} \in G_2, \varphi(h) \in H_2$. 而

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(h)(\varphi(g))^{-1} \in H_2$$故$ghg^{-1} \in \varphi^{-1}(H_2)$，即$\varphi^{-1}(H_2)$是$G_1$的正规子群.

6　证　设G是单群，G'是G的同态象，N是同态核，则N是G的正规子群，由G是单群，故N或是恒等元群$\{e\}$或是G.

若$N = \{e\}$，则$G = G/\{e\} \cong G'$，故G'为单群；

若$N = G$，则$\{G\} = G/G \cong G'$，故G'为恒等元群.

7　证　由同态基本定理知，群G的任一同态象必同构于其商群，而商群完全由G和G的正规子群所决定.已知Z_{12}为循环群，它有且只有6个子群（见§4习题12），显然皆为正规子群.

$H_1 = \{\bar{0}\} = (\bar{0})$，$H_2 = \{\bar{0}, \bar{6}\} = (\bar{6})$，$H_3 = \{\bar{0}, \bar{4}, \bar{8}\} = (\bar{4})$，$H_4 = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} = (\bar{3})$，$H_5 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\} = (\bar{2})$，$H_6 = Z_{12}$

由$G = Z_{12}$和其正规子群决定的商群为

$G/H_1 = G = Z_{12}, G/H_2 = \{H_2, \bar{1} + H_2, \bar{2} + H_2, \bar{3} + H_2, \bar{4} + H_2, \bar{5} + H_2\} = (\bar{1} + H_2) \cong Z_6, G/H_3 = \{H_3, \bar{1} + H_3, \bar{2} + H_3, \bar{3} + H_3\} = (\bar{1} + H_3) \cong Z_4, G/H_4 = \{H_4, \bar{1} + H_4, \bar{2} + H_4\} = (\bar{1} + H_4) \cong Z_3$，$G/H_5 = \{H_5, \bar{1} + H_5\} \cong Z_2$，$G/H_6 = \{Z_{12}\} \cong \{\bar{0}\}$.

从同构观点看，Z_{12}的所有同态象即它的所有商群，共有6个都是循环群。

已知$G=S_3$共有6个子群（见§6正文）：

$H_1=\{(1)\},H_2=\{(1),(12)\},H_3=\{(1),(13)\}$

$H_4=\{(1),(23)\},H_5=\{(1),(123),(132)\},H_6=S_3$

其中只有H_1,H_5,H_6为S_3的正规子群，故S_3的同态象（从同构观点看）有且只有3个为

$$S_3,\ S_3/H_5=\{H_5,(12)H_5\}\cong Z_2,H_1$$

8 证 设$n_2\backslash n_1$，$n_1=n_2q$，因G_1是循环群，故G_1有q阶子群H，且H是正规子群。G_1/H是n_2阶循环群。而G_2也是n_2阶循环群，故有$\varphi:G_1/H\cong G_2$。另外，存在G_1到G_1/H的自然同态 f：$G_1\sim G_1/H$。令$\psi=\varphi f$，则有$\psi:G_1\sim G_2$。

反之，若$G_1\overset{\psi}{\sim}G_2$，$\psi$的核为$N$。由同态基本定理知$G_1/N\cong G_2$，于是$G_1/N$的阶数为$n_2$，即$N$在$G_1$中的指数为$n_2$，故$n_2\backslash n_1$。

9 证 $\forall H\in A$，因H是G的子群，所以$\varphi(H)$是G'的子群。故$\varphi:H\longmapsto\varphi(H)$是$A$到$A'$的映射。

$\forall H'\in A'$，令$H=\varphi^{-1}(H')=\{x\in G\mid\varphi(x)\in H'\}$ 则H是G的子群，且$H\supseteq K$。因为$\forall k\in K$，有$\varphi(k)=e'\in H'\Longrightarrow k\in H\Longrightarrow k\subseteq H$。即$H$是$G$的含有$K$的子群，$H\in A,\varphi(H)=H'$，从而$\varphi$是$A$到$A'$的满射。

由本节习题3知当$H\supseteq K$时，有$\varphi^{-1}(\varphi(H))=H$。设$H_1,H_2$是$A$中两个元，$H_1\neq H_2$，则$\varphi(H_1)\neq\varphi(H_2)$，如果$\varphi(H_1)=\varphi(H_2)$，那么$\varphi^{-1}(\varphi(H_1))=\varphi^{-1}(\varphi(H_2))$，于是$H_1=H_2$。矛盾。故$\varphi$是$A$到$A'$的双射。

由本节习题5知若H是G的正规子群，则$\varphi(H)$是G'的正规子群。反之，若$\varphi(H)=H'$是G'的正规子群。因为$H\supseteq K$，故$\varphi^{-1}(\varphi(H))=\varphi^{-1}(H')=H$，因此$H$是$G$的正规子群。

10 证 设$\overline{H}$为G/N的任一子群，$G\overset{\varphi}{\sim}G/N$为自然同态，

其核为N。则$\overline{H}$的完全原象$H=\varphi^{-1}(\overline{H})$是$G$的子群，且$H\supseteq N$。显然$N$也是$H$的正规子群，且$\overline{H}=\varphi(H)=\{aN|a\in H\}=H/N$。即$G/N$的任一子群均具有这种形式。

11　**证**　令φ为G到G/N的自然同态，核为N.因$K\supseteq N$，故$\varphi(K)=K/N$，由于K是G的正规子群,故$\varphi(K)=K/N$是G/N的正规子群，又$\varphi^{-1}(\varphi(K))=\varphi^{-1}(K/N)=K$（因$K\supseteq N$），利用§ 8 例3的结论有

$$(G/N)/(K/N)\cong G/K$$

12　**证**　由§ 7 习题 7 知KN是G的正规子群，且$KN\supseteq N$。在上题中用KN代替K，即得所求。

13　**证**　令

$$\varphi: n\longmapsto a^n$$

显然φ是整数加群Z到循环群(a)的满射，而且

$$\varphi(n_1+n_2)=a^{n_1+n_2}=a^{n_1}a^{n_2}=\varphi(n_1)\varphi(n_2)$$

故φ是Z到(a)的一个同态映射。

设φ的核为$N=\varphi^{-1}(e)$。当a的阶为无限时，若$a^m=e$，只有$m=0$.所以$N=(0)$；此时$Z/(0)=Z\cong(a)$（此处将$Z/(0)$看作Z）；当a的阶为n时，即n为使$a^n=e$的最小正整数，而且$a^k=e$，当且仅当$k=nq$。即$N=(n)$。于是$Z/(n)\cong(a)$，即$Z_n\cong(a)$。

14　**证**　证明的基本思路是:假如G还有一个阶数为n的子群K,我们希望证明$K=N$.如果能证得$K\subseteq N$,当然就有$K=N$。而若$K\subseteq N$时，就有$NK=N$，反之亦然。所以证明的关键是如何证明$NK=N$.。而证$NK=N$可以转化为证明NK/N的阶数为1。为此，我们考虑NK/N。因N是G的正规子群，所以NK是G的子群且含有N.由§ 8 习题10知NK/N有意义且NK/N是商群G/N的子群。由题给条件N在G中的指数为m，即商群G/N的阶为m。设NK/N的阶为t，则$t|m$。由例题选讲中例

10的结论知

$$NK/N \cong K/K \cap N$$

故$K/K \cap N$的阶也为 t，但K的阶为n，故$t \backslash n$。于是$t \backslash (m,n)$，因$(m,n)=1$，故$t=1$，即$NK=N$。故$K=N$。

§9

1　证　若$G_1+G_2=G_1 \oplus G_2$，则$\forall a+b \in G_1+G_2$；$a \in G_1$，$b \in G_2$。那么，对于$c \in G_1 \cap G_2$，便有$(a+c)+b=a+(c+b) \in G_1 \oplus G_2$，其中$a+c \in G_1, b \in G_2$；$a \in G_1, c+b \in G_2$，由直和元素表法唯一，知$a+c=a$，从而知$c=0$，故$G_1 \cap G_2=\{0\}$。

反之，若$G_1 \cap G_2=\{0\}$，且$a_1+b_1=a_2+b_2 \in G_1+G_2$。其中$a_1,a_2 \in G_1, b_1,b_2 \in G_2$，于是有$a_1-a_2=b_1-b_2$。$a_1-a_2 \in G_1, b_1-b_2 \in G_2$，故得$a_1-a_2=b_1-b_2 \in G_1 \cap G_2=\{0\}$。从而有$a_1=a_2, b_1=b_2$，即$G_1+G_2$中元素表法唯一，故$G+G_2=G_1 \oplus G_2$。

2　证　G_1与G_2的（外）直和为

$\overline{G}=\{(\overline{0},\overline{0}),(\overline{0}\ \ \overline{2}),(\overline{0},\overline{4}),(\overline{3},\overline{0}),(\overline{3},\overline{2}),(\overline{3},\overline{4})\}$

G_1与G_2的（内）直和为

$$G=\{\overline{0}+\overline{0}=\overline{0},\ \overline{0}+\overline{2}=\overline{2},\ \overline{0}+\overline{4}=\overline{4},$$
$$\overline{3}+\overline{0}=\overline{3},\ \overline{3}+\overline{2}=\overline{5},\ \overline{3}+\overline{4}=\overline{1}\}$$

令　$\varphi:\overline{G} \longrightarrow G,\ (\overline{a},\overline{b}) \longmapsto \overline{a}+\overline{b}=\overline{a+b}$

下证φ是$\overline{G}$到G的同构映射。

若　$\varphi(\overline{a},\overline{b})=\varphi(\overline{a}_1,\overline{b}_1)$，即$\overline{a}+\overline{b}=\overline{a}_1+\overline{b}_1$，于是

$\overline{a}-\overline{a}_1=\overline{b}_1-\overline{b} \subset G_1 \cap G_2=\{\overline{0}\}$，故$\overline{a}_1=\overline{a}$，$\overline{b}_1=\overline{b}$。从

而知 $(\overline{a}, \overline{b}) = (\overline{a}_1, \overline{b}_1)$. 故 φ 是单射.

$\forall \overline{x} \in G$, 皆可表为 $\overline{x} = \overline{a} + \overline{b}$, $\overline{a} \in G_1$, $\overline{b} \in G_2$. 于是有 $(\overline{a}, \overline{b}) \in \overline{G}$, 使 $\varphi(\overline{a}, \overline{b}) = \overline{x}$. 从而知 φ 是满射. 且

$\varphi((\overline{a}_1, \overline{b}_1) + (\overline{a}_2, \overline{b}_2)) = \varphi(\overline{a_1 + a_2}, \overline{b_1 + b_2}) = \overline{a_1 + a_2} + \overline{b_1 + b_2} = \overline{a_1 + b_1} + \overline{a_2 + b_2} = \varphi(\overline{a}_1, \overline{b}_1) + \varphi(\overline{a}_2, \overline{b}_2)$. 故 φ 是同构映射. 于是 $\overline{G} \cong G$.

3 证 令 $\varphi: G_1 \longrightarrow G_1 \oplus G_2 / \overline{G}_2$

$$a \longmapsto (a, 0) + \overline{G}_2 \quad \forall a \in G_1$$

可证 φ 是 G_1 到 $G_1 \oplus G_2 / \overline{G}_2$ 的同构映射.

4 证 令 $\varphi: G_1 \longrightarrow G_1 \oplus G_2 / G_2$

$a \longmapsto (a + g_2) + G_2 = a + G_2 \quad g_2 \in G_2$ 即可证出.

第三章　环与域习题解答

§1

1　证　由§1环的性质（2）得

$$(-a)(-b)=-(a(-b))=-(-ab)=ab$$

2　证　设R是有1的环，G是R中所有可逆元的集合。现证明G对于R的乘法封闭。

$\forall a,b\in G$，因存在$a^{-1},b^{-1}\in R$，有$(ab)^{-1}=b^{-1}a^{-1}\in R$，即$ab$是$R$的可逆元，故$ab\in G$。群的其它条件显然成立。

3　证　$\forall a, b_1,b_2,\cdots,b_n\in R$，证明

$$a\cdot(b_1+b_2+\cdots+b_n)=(a\cdot b_1)+(a\cdot b_2)+\cdots+(a\cdot b_n) \tag{1}$$

$$(b_1+b_2+\cdots+b_n)\cdot a=(b_1\cdot a)+(b_2\cdot a)+\cdots+(b_n\cdot a) \tag{2}$$

对n用数学归纳法。

当$n=2$时，由分配律得$a\cdot(b_1+b_2)=(a\cdot b_1)+(a\cdot b_2)$

假设（1）式对于$n-1$成立，则由结合律、分配律得

$$\begin{aligned}a\cdot(b_1+b_2+\cdots+b_n)&=a\cdot((b_1+b_2+\cdots+b_{n-1})+b_n)\\&=(a\cdot(b_1+b_2+\cdots+b_{n-1}))+(a\cdot b_n)\\&=((a\cdot b_1)+(a\cdot b_2)+\cdots+(a\cdot b_{n-1}))+(a\cdot b_n)\\&=(a\cdot b_1)+(a\cdot b_2)+\cdots+(a\cdot b_n)\end{aligned}$$

（1）式得证。类似可证（2）。

4　证　用反证法。设$a\in R$，$a\neq 0$。假设，$1=0$，则由§1

环的性质（1）知

$$a\cdot 1=a\cdot 0=0\neq a$$

与单位元的性质矛盾．故必有$1\neq 0$.

5　**解**　例如，偶数环就无单位元．

6　**证**（1）$\forall(x_1,x_2),(y_1,y_2)\in R$，由 $x_1,y_1\in R_1$，$x_2,y_2\in R_2$ 知 x_1+y_1，$x_1y_1\in R_1$，x_2+y_2，$x_1y_2\in R_2$，从而

$$(x_1,x_2)+(y_1,y_2)=(x_1+y_1,x_2+y_2)\in R$$

$$(x_1,x_2)(y_1,y_2)=(x_1y_1,x_2y_2)\in R$$

即R对所规定的加法和乘法封闭．

其次，$\forall(x_1,x_2),(y_1,y_2),(z_1,z_2)\in R$，由$R_1$，$R_2$的加法、乘法结合律得

$$((x_1,x_2)+(y_1,y_2))+(z_1,z_2)=(x_1+y_1,x_2+y_2)+(z_1,z_2)$$
$$=((x_1+y_1)+z_1,(x_2+y_2)+z_2)=(x_1+(y_1+z_1),x_2+(y_2+z_2))$$
$$=(x_1,x_2)+(y_1+z_1,y_2+z_2)=(x_1,x_2)+((y_1,y_2)+(z_1,z_2))$$

$$((x_1,x_2)\cdot(y_1,y_2))\cdot(z_1,z_2)=(x_1\cdot y_1,x_2\cdot y_2)\cdot(z_1,z_2)$$
$$=((x_1\cdot y_1)\cdot z_1,(x_2\cdot y_2)\cdot z_2)=(x_1\cdot(y_1\cdot z_1),x_2(y_2\cdot z_2))$$
$$=(x_1,x_2)\cdot((y_1\cdot z_1,y_2\cdot z_2)=(x_1,x_2)\cdot((y_1,y_2)\cdot(z_1,z_2))$$

即R的加法和乘法都满足结合律．从而$\{R;\ +\}$和$\{R;\ \cdot\}$都是半群．

设0_1和0_2分别是R_1和R_2的零元，则$(0_1,0_2)$是R的零元：$\forall(x_1,x_2)\in R$有

$$(x_1,x_2)+(0_1,0_2)=(x_1+0_1,x_2+0_2)=(x_1,x_2)$$

$\forall(x_1,x_2)\in R$，则$(-x_1,-x_2)\in R$是(x_1,x_2)的负元

$$(x_1,x_2)+(-x_1,-x_2)=(x_1-x_1,x_2-x_2)=(0_1,0_2)$$

同时易证R的加法满足交换律．于是$\{R;+\}$是交换群．

最后证明乘法对加法满足分配律．$\forall(x_1,x_2)$，(y_1,y_2)，$(z_1,z_2)\in R$，有

$$(x_1,x_2)\cdot((y_1,y_2)+(z_1,z_2))=(x_1,x_2)\cdot(y_1+z_1,y_2+z_2)$$
$$=(x_1\cdot(y_1+z_1),x_2\cdot(y_2+z_2))=(x_1y_1+x_1z_1,x_2y_2+x_2z_2)$$

$$= (x_1y_1, x_2y_2) + (x_1z_1, x_2z_2) = ((x_1, x_2)\cdot(y_1, y_2)) + ((x_1, x_2)\cdot(z_1, z_2))$$

类似地可证

$$((y_1, y_2) + (z_1, z_2))\cdot(x_1, x_2) = ((y_1, y_2)\cdot(x_1, x_2)) + ((z_1, z_2)\cdot(x_1, x_2))$$

综上所述，$\{R; +, \cdot\}$是环。

（2）假设R是交换环。$\forall x_1, y_1 \in R_1, \forall x_2, y_2 \in R_2$，由于

$$(x_1, x_2)(y_1, y_2) = (y_1, y_2)(x_1, x_2)$$

而有

$$(x_1y_1, x_2y_2) = (y_1x_1, y_2x_2)$$

由R元素的相等条件得

$$x_1y_1 = y_1x_1, \quad x_2y_2 = y_2x_2$$

即R_1和R_2都是交换环。

反之，假设R_1和R_2都是交换环，易证R是交换环。

（3）$\forall (x_1, x_2) \in R$，则

$$(x_1, x_2)(e_1, e_2) = (x_1e_1, x_2e_2) = (x_1, x_2)$$

$$(e_1, e_2)(x_1, x_2) = (e_1x_1, e_2x_2) = (x_1, x_2)$$

故 $e = (e_1, e_2)$是R的单位元。

设$a = (a_1, a_2) \in R$有逆元$a^{-1} = (a_1', a'_2) \in R$，则

$$(a_1a_1', a_2a_2') = aa^{-1} = (e_1, e_2)$$

$$(a_1'a_1, a_2'a_2) = a^{-1}a = (e_1, e_2)$$

从而

$$a_1a_1' = a_1'a_1 = e_1, \quad a_2a_2' = a_2'a_2 = e_2$$

即a_1'和a_2'分别是a_1和a_2的逆元。

反之，假设a_1和a_2分别有逆元$a_1^{-1} \in R_1$和$a_2^{-1} \in R_2$，则$(a_1^{-1}, a_2^{-1}) \in R$是$(a_1, a_2)$的逆元：

$$(a_1, a_2)(a_1^{-1}, a_2^{-1}) = (a_1a_1^{-1}, a_2a_2^{-1}) = (e_1, e_2)$$

$$(a_1^{-1}, a_2^{-1})(a_1, a_2) = (a_1^{-1}a_1, a_2^{-1}a_2) = (e_1, e_2)$$

7　证　$\forall f, g \in R$，则 $f+g, fg$ 也都是〔0, 1〕上的实函

数，即 $f+g$，$fg\in R$. 由函数性质知，函数加法和乘法都满足结合律、交换律，乘法对加法满足分配律. 此外，零函数

$$f_0\equiv 0$$

是 R 中的零元. $\forall f\in R$, 有负函数 $-f\in R$. 因此 R 关于函数加法和乘法构成环。

8 证 $\forall a\in R$, 有 $ea=a$。此时，R 的元素 $ae-a+e$ 也是 R 的左恒等元. 事实上，$\forall b\in R$

$$(ae-a+e)b=aeb-ab+eb=ab-ab+b=b$$

由于左恒等元是唯一的，则有

$$ae-a+e=e, ae=a$$

即 e 也是 R 的右恒等元，从而是恒等元.

9 证 由于 a' 是 a 的左逆元：$a'a=1$, 则 $aa'-1+a'$ 也是 a 的左逆元：

$$(aa'-1+a')a=aa'a-a+a'a=a-a+a'a=1$$

因 a 的左逆元是唯一的，故

$$aa'-1+a'=a', aa'=1$$

即 a' 也是 a 的右逆元，从而是 a 的逆元。

10 证 因存在正整数 n 使 $a^n=0$，则 $1+a+a^2+\cdots+a^{n-1}\in R$ 是 $1-a$ 的逆元。这是因为：

$$(1-a)(1+a+a^2+\cdots+a^{n-1})=1-a^n=1, (1+a+a^2+\cdots+a^{n-1})(1-a)=1-a^n=1$$

故$1-a$是可逆元。

§2

1 证 设 a 是 R 的可逆元，如果对于 $b\in R$ 有

$$ab=0$$

两端左乘 a^{-1}，得 $b=0$, 这说明 a 不是零因子.

2 证 由 $a^2=a$ 得 $a^2-a=0, a(a-1)=0$，因 $a\neq 0$ 且 R 是整环，故 $a-1=0$，即 $a=1$。

这个结论不是在任意环中都成立的．例如，在Z_6中$\overline{3}^2=\overline{3}\neq 1$。

3 解 $R[x]$ 中，零次多项式都是可逆元．次数大于零的多项式都不是可逆元．所以 $R[x]$不是域。

4 证 必要性．设R是整环．$\forall a,b\in \dot{R}$，由于R无真零因子，则 $ab\neq 0$，即$ab\in \dot{R}$)．从而$\dot{R}$是R的乘法子半群。

充分性．设$\{\dot{R};\cdot\}$是$\{R;\cdot\}$的子半群，则对于R的任意两个非零元a，b（即a，$b\in\dot{R}$）有$ab\in\dot{R}$，即 $ab\neq 0$，从而R无真零因子，R是整环。

5 证 必要性．设R无真左零因子．如 $ax=ay$，$a\neq 0$，则 $ax-ay=0, a(x-y)=0, x-y=0, x=y$。

充分性．假设左消去律成立．$\forall a(\neq 0)\in R$，如果$b\in R$使$ab=0$，则$a\cdot b=a\cdot 0$．由左消去律得 $b=0$，这说明a不是真零因子，从而R无真零因子．对于真右零因子和右消去律的情形，证明方法类似。

6 证 由 $n>1$ 知$\dot{R}$是$n-1$个元素的非空集合．由题设知，$\{\dot{R};\cdot\}$是半群．由习题5知，乘法消去律成立．再由第二章有限群的判定定理知 $\{\dot{R};\cdot\}$是群．从而R是除环。

7 证 只需证明S对于乘法封闭．$\forall a,b\in S$，有 $ab\neq 0$。如果 $c\in R$ 使

$$(ab)c=0,\quad a(bc)=0$$

因a不是零因子，故$bc=0$．因b不是零因子，故$c=0$。这说明ab不是零因子，即$ab\in S$，从而$\{S;\cdot\}$是半群。

8 证 用反证法．假设$\varphi:\{R;+\}\cong\{\dot{R};\cdot\}$，则 $\varphi(0)=1$．设$\varphi^{-1}(-1)=a$，即 $\varphi(a)=-1$。

当 $a=0$，则 $1=-1$；当 $a\neq 0$，则$\varphi(a+a)=\varphi(a)\varphi(a)=(-1)(-1)=1$．于是，$a+a=0, a(1+1)=0$得到$1+1=0$，即$1=-1$．总之，无论哪种情况，均有$1=-1$。

于是

$$\varphi(1)\varphi(1)=\varphi(1+1)=\varphi(1+(-1))=\varphi(0)=1$$

$$\varphi(1)\varphi(1)-1=0,\ (\varphi(1)-1)^2=0,\quad (\because\ 1=-1)$$

$$\varphi(1)-1=0,\ \varphi(1)=1$$

但在除环中，$1\neq0$，故此结果与$\varphi(0)-1$相矛盾．所以在$\{R;+\}$与$\{\dot{R};\cdot\}$之间不存在同构映射φ．

9 证 必要性．设R是除环，则$\{\dot{R};\cdot\}$是群．于是，$\forall a,b\in R$，当$a\neq0,b\neq0$时，有$a,b\in\dot{R}$，方程$ax=b$在$\dot{R}$中（自然在R中）有解．当$a\neq0$，$b=0$时，方程$ax=0$有解$x=0\in R$．

充分性．设$\forall a\ (\neq0)$，$b\in R$，方程$ax=b$在R中有解．$\forall a',b'\in\dot{R}$，则$a'x=b'$有解$x=c\in R$；方程$b'y=c$有解$y=d\in R$．于是$a'b'd=b'$．由于$b'\neq0$，所以$a'b'\neq0$，即$a'b'\in\dot{R}$．这既说明$\dot{R}$对乘法封闭，又说明R无真零因子．由习题5，消去律成立．

其次，由$R\neq\{0\}$知，存在$a\in\dot{R}$．方程$ax=a$，有解$x=e\in\dot{R}$．因为$ae=a$，$ae^2=ae$．由消去律$e^2=e$．

$\forall b\in\dot{R}$，以b左乘上式两端$be^2=be$，再由消去律得$be=b$．

最后，$\forall a\in\dot{R}$，方程$ax=e$，有解$x=a'\in\dot{R}$：$aa'=e$．

综上所述，$\{\dot{R};\cdot\}$是群，从而R是除环．

10 证 设R的元素个数为n，$a\in R$不是R的可逆元，则R中没有元素x使$ax=1$．考虑集合$S=\{ar\mid r\in R\}$．由于$1\bar{\in}S$，故S是R的真子集，S的元素个数小于n．但形如ar的乘积可写出n个．因此必存在r_1，$r_2\in R$，$r_1\neq r_2$使得

$$ar_1=ar_2,\ a(r_1-r_2)=0$$

其中$r_1-r_2\neq0$．说明a是左零因子．

同理可证a是右零因子．由此，当R是有限整环时，R无真零因子，所以R的每个非零元都必是可逆元，从而$\{\dot{R};\cdot\}$是可换群，于是R是域．

§3

1 证 显然S非空．$\forall\alpha,\beta\in S$，$\alpha=a_1+b_1i$，$\beta=a_2+b_2i$，

$a_i, b_i \in \mathbf{Z}$, 则

$$\alpha-\beta=(a_1-a_2)+(b_1-b_2)i, \alpha\beta=(a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i$$

其中 a_1-a_2, b_1-b_2, $a_1a_2-b_1b_2$, $a_1b_2+a_2b_1\in \mathbf{Z}$, 故 $\alpha-\beta, \alpha\beta\in S$. 由定理 1 之（4）知 S 是C的子环.

利用定理 2 之（4）可验证K是C的子域.

2　证　显然S非空. $\forall f(x^2)$, $g(x^2)\in S$, $f(x)$, $g(x)\in \mathbf{R}[x]$, 因$f(x)-g(x)$, $f(x)g(x)\in \mathbf{R}[x]$, 故$f(x^2)-g(x^2), f(x^2)g(x^2)\in S$, 从而 S 是 $\mathbf{R}[x]$的子环.

3　证　$\forall \alpha,\beta\in S[a_1,a_2,\cdots,a_n]$; $\alpha=\sum c_{k_1k_2\cdots k_n}a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n}$

$\beta=\sum c'_{h_1h_2\cdots h_n}a_1^{h_1}a_2^{h_2}\cdots a_n^{h_n}$, 其中 $c_{k_1k_2\cdots k_n}, c'_{h_1h_2\cdots h_n}\in S$. 则

$$\alpha-\beta=\sum c_{k_1k_2\cdots k_n}a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n}+\sum(-c'_{h_1h_2\cdots h_n})a_1^{h_1}a_2^{h_2}\cdots a_n^{h_n} \quad (1)$$

$$\alpha\beta=\sum c_{k_1k_2\cdots k_n}\cdot c'_{h_1h_2\cdots h_n}a_1^{k_1+h_1}a_2^{k_2+h_2}\cdots a_n^{k_n+h_n} \quad (2)$$

由于S是环, $-c'_{h_1h_2\cdots h_n}$和$c_{k_1k_2\cdots k_n}\cdot c'_{h_1h_2\cdots h_n}$都是$S$中的元素，所以（1）和（2）都是满足$S[a_1,a_2,\cdots,a_n]$的条件的有限和，故有$\alpha-\beta, \alpha\beta\in S[a_1,a_2,\cdots,a_n]$, 从而$S[a_1,a_2,\cdots,a_n]$是$R$的子环.

显然$S\subseteq S[a_1,a_2,\cdots,a_n]$; $a_1,a_2,\cdots,a_n\in S[a_1,a_2,\cdots,a_n]$. 设$\overline{S}$是满足条件: $S\subseteq\overline{S}$, $a_1,a_2,\cdots,a_n\in\overline{S}$的$R$的任意子环. $\forall\alpha=\sum c_{k_1k_2\cdots k_n}a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n}\in S[a_1,a_2,\cdots,a_n]$, 因$c_{k_1k_2\cdots k_n}, a_1,a_2,\cdots, a_n\in\overline{S}$, 则$c_{k_1k_2\cdots k_n}a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n}\in\overline{S}$, 从而　$\alpha\in\overline{S}$. 因此 $S[a_1,a_2,\cdots,a_n]\subseteq\overline{S}$.

4　证　由习题3知$Z[i]=\{\sum c_k i^k \mid c_k\in Z\}$. 显然$S\subseteq Z[i]$.

另一方面，由习题 1，S是 C 的子环. 而且 $\forall n\in Z$ 有$n=$

$n+0\cdot i\in S$　以及 $i=0+1\cdot i\in S$，依习题 3 最后的结论知 $Z[i]\subseteq S$。故

$$S=Z[i].$$

类似可证　$K=Q[i]$。

5　证　由习题 3 知 $S\subseteq S[a_1,a_2]$，且 $a_1,a_2\in S[a_1,a_2]$，于是 $S[a_1]\subseteq S[a_1,a_2]$，从而 $S[a_1][a_2]\subseteq S[a_1,a_2]$。

反之，由于 $S\subseteq S[a_1]$，且 $S[a_1]\subseteq S[a_1][a_2]$，有 $S\subseteq S[a_1][a_2]$。同时，由 $a_1\in S[a_1]$ 知 $a_1\in S[a_1][a_2]$，$a_2\in S[a_1][a_2]$，故由习题 3 知：$S[a_1,a_2]\subseteq S[a_1][a_2]$，因此 $S[a_1,a_2]=S[a_1][a_2]$。

6　解　由高等代数知，n 阶方阵 A 与每个 n 阶方阵 X 可换：$AX=XA\Longleftrightarrow A$ 是纯量阵，$A=kE_n$，故 $M_2(C)$ 的中心是

$$C=\{kE_2 \mid k\in C\}$$

7　证　显然 $0\in C(S)$，$C(S)$ 非空。

$\forall r_1, r_2\in C(S)$，$\forall x\in S$，则

$$(r_1-r_2)x=r_1x-r_2x=xr_1-xr_2=x(r_1-r_2)$$

$$(r_1r_2)x=r_1(r_2x)=r_1(xr_2)=(r_1x)r_2=(xr_1)r_2=x(r_1r_2)$$

即 $r_1-r_2, r_1r_2\in C(S)$。因此 $C(S)$ 是 R 的子环。

8　证（1）由 $a^2=a$ 知，$\forall x\in R$

$$\begin{aligned}(axa-ax)^2&=axaaxa-axaxa-axaax+axax\\&=axa^2xa-axaxa-axa^2x+axax\\&=axaxa-axaxa-axax+axax=0\end{aligned}$$

因 R 中无非零幂零元，故

$$axa-ax=0$$

同理可证

$$axa-xa=0$$

由上述两式推得 $ax=xa$。

（2）设 S 是 R 的所有幂零元素集合。由 $0\in S$ 知 S 非空。$\forall a,b\in S$，$a^m=0$，$b^n=0$ 则

$$(a-b)^{m+n}=a^{m+n}-C_{m+n}^{1}a^{m+n-1}b+\cdots$$
$$+(-1)^{i}C_{m+n}^{i}a^{m+n-i}b^{i}+\cdots+(-1)^{m+n}b^{m+n}=0$$
$$(ab)^{mn}=a^{mn}b^{mn}=0$$

即 $a-b$，ab 都是R的幂零元，故 $a-b$，$ab\in S$，S 是R的子环。

9　证　因$p\nmid 1$，故 $\mathbf{Z}\subset S_p$，说明 S_p 非空。$\forall\alpha,\beta\in S_p$：$\alpha=\dfrac{a_1}{b_1}$，　$\beta=\dfrac{a_2}{b_2}$，$a_1,a_2,b_1,b_2\in\mathbf{Z}$，$p\nmid b_1$，$p\nmid b_2$，则$\alpha-\beta=\dfrac{a_1}{b_1}-\dfrac{a_2}{b_2}=\dfrac{a_1b_2-a_2b_1}{b_1b_2}$，$\alpha\beta=\dfrac{a_1}{b_1}\cdot\dfrac{a_2}{b_2}=\dfrac{a_1a_2}{b_1b_2}$

上述两式右端的分子、分母都是整数，而且，$p\nmid b_1b_2$，故 $\alpha-\beta$，$\alpha\beta\in S_p$，S_p 是$\mathbf{Q}$的子环。

§4

1　证　因R不是零乘环，存在 $a,b\in R$ 使
$$ab\neq 0$$
又因 $n>1$，故 $M_n(R)$中存在

$$\boldsymbol{A}=\begin{pmatrix}0&a&0&\cdots&0\\0&0&0&\cdots&0\\\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&0&\cdots&0\end{pmatrix},\quad \boldsymbol{B}=\begin{pmatrix}0&0&0&\cdots&0\\0&b&0&\cdots&0\\\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&0&\cdots&0\end{pmatrix}$$

于是

$$\boldsymbol{AB}=\begin{pmatrix}0&ab&0&\cdots&0\\0&0&0&\cdots&0\\\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&0&\cdots&0\end{pmatrix}\neq 0$$

而　$\boldsymbol{BA}=0$，因此 $M_n(R)$不是交换环。

2　解　$\det\boldsymbol{A}=1$ 是 $\mathbf{Z}$ 中可逆元．由定理知$\boldsymbol{A}$有逆阵，其

逆阵是

$$A^{-1}=(\det A)^{-1}\widetilde{A}=1\cdot\widetilde{A}=\widetilde{A}=\begin{pmatrix}-14 & 45 & -5\\ 3 & -9 & 1\\ 3 & -10 & 1\end{pmatrix}$$

$\det B=2$不是$\boldsymbol{Z}$中的可逆元，故B在$M_3(\boldsymbol{Z})$中无逆阵。

3　**解**　A在$M_n(R)$中有逆阵，必要而且只要$a_1a_2\cdots a_n$是R中的可逆元，必要而且只要每个a_i是可逆元。

4　**证**　必要性　设A是$M_n(F)$中的零因子，则存在$B(\neq 0)\in M_n(F)$使得$AB=0$。假设A有逆阵$A^{-1}\in M_n(F)$，以A^{-1}左乘上式两端得$B=0$，矛盾。故A在$M_n(F)$中无逆阵。

充分性　假设A在$M_n(F)$中无逆阵，由本节推论1有

$$\det A=0$$

于是存在可逆阵$P,Q\in M_n(F)$，使得

$$PAQ=\begin{pmatrix}1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0\end{pmatrix}=D_r,\quad r<n$$

（其中1共r个）

用

$$S=\begin{pmatrix}0 & & & \\ & \ddots & & \\ & & 0 & \\ & & & 1\end{pmatrix}$$

右乘上式两端得$PAQS=0$。

用P^{-1}左乘上式两端得$AQS=0$。由本题的第一部分（必要性）知

$$QS\neq 0$$

故A是左零因子。同理可证A是右零因子。从而A是零因子。

这个结论对一般的有1交换环R不成立。例如，$R=\boldsymbol{Z}$，在$M_2(\boldsymbol{Z})$中，方阵

$$\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$$

既无逆阵也不是零因子。

5 解 (1) 因为 $|E_n+pE_{ij}|=1$ 是 R 中可逆元，故 E_n+pE_{ij} 在 $M_n(R)$ 中有逆元。

(2) 因 $|E_n+(p-1)E_{ii}|=p$，故当 P 是 R 中可逆元时，$E_n+(p-1)E_{ii}$ 是 $M_n(R)$ 中的可逆元。

(3) 用 E_n+pE_{ij} 左乘 A 等于把 A 的第 j 行左乘 P 加到 A 的第 i 行。用 E_n+pE_{ij} 右乘 A 等于把 A 的第 i 列右乘 P 加到 A 的第 j 列。用 $E_n+(p-1)E_{ii}$ 左乘 A 等于用 p 左乘 A 的第 i 行。用 $E_n+(p-1)E_{ii}$ 右乘 A 等于用 p 右乘 A 的第 i 列。

6 与高等代数中行列式的有关结果的证明相同。

7 解 本节最后的例中，$M_2(Z_2)$ 的子环

$$S=\left\{\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \middle|\ x,y\in Z_2\right\}$$

是恰含四个元素的无单位元的非交换环。

§5

1 证 $\forall\begin{pmatrix} a_1 & 0 \\ a_2 & 0 \end{pmatrix}, \begin{pmatrix} a_1' & 0 \\ a_2' & 0 \end{pmatrix}\in N_1$，$\begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix}\in M_2(R)$；有

$$\begin{pmatrix} a_1 & 0 \\ a_2 & 0 \end{pmatrix}-\begin{pmatrix} a_1' & 0 \\ a_2' & 0 \end{pmatrix}=\begin{pmatrix} a_1-a_1' & 0 \\ a_2-a_2' & 0 \end{pmatrix}\in N_1$$

$$\begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix}\begin{pmatrix} a_1 & 0 \\ a_2 & 0 \end{pmatrix}=\begin{pmatrix} x_1a_1+x_3a_2 & 0 \\ x_2a_1+x_4a_2 & 0 \end{pmatrix}\in N_1$$

故 N_1 是 $M_2(R)$ 的左理想，但不是右理想。例如，$\forall\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\in N_1$，$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\in M_2(R)$，有

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\overline{\in} N_1$$

同理可证 N_2 是 $M_2(R)$ 的右理想，但不是左理想。N_1, N_2 都不是双边理想。

2 证 设 I 和 J 是 R 的左理想。

$\forall\ a=u_1+v_1,\ b=u_2+v_2\in I+J,\ u_i\in I,\ v_i\in J$，及$\forall r\in R$ 有

$$a-b=(u_1+v_1)-(u_2+v_2)=(u_1-u_2)+(v_1-v_2)\in I+J$$

$$ra=r(u_1+v_1)=ru_1+rv_1\in I+J$$

所以 $I+J$ 是R的左理想．同理可证，当I,J 是右（双边）理想时，$I+J$ 是右（双边）理想．

3　**解**　假设$(a)=(b)$．当$a=0$，显然有$b=0$．当$a\neq0$，由 $a\in(b)$及 $b\in(a)$ 得

$$a=rb,\ b=r'a,\ r,r'\in R$$

于是

$$a=rr'a\ \text{即}(rr'-1)a=0$$

由于R是整环，则

$$rr'-1=0\quad\text{即}\quad rr'=1$$

即 r 是可逆元．所以，当$(a)=(b)$时，必有 $a=rb$，其中 r 是 R中的可逆元．

反之，如果 $a=rb$，r 是可逆元，易证 $(a)=(b)$．

因此，$(a)=(b)$的充分必要条件是 $a=rb$，r 是可逆元．

4　**解**　参见例10，可求得 $Z[i]/N$ 的元素个数为 n^2．

5　**解**　$x+1$ 和 $x-1$ 都是 $F[x]$ 中的元素，因 x^2-1 不能整除 $x+1$ 和 $x-1$，所以 $x+1$，$x-1\overline{\in}(x^2-1)$，即它们所在的类

$$\overline{x+1}\neq\overline{0},\quad\overline{x-1}\neq0$$

但

$$\overline{x+1}\cdot\overline{x-1}=\overline{(x+1)(x-1)}=\overline{x^2-1}=\overline{0}$$

这说明$\overline{x+1}$和$\overline{x-1}$都是真零因子，故 $F[x]/(x^2-1)$不是整环．

6　**证**　显然$(1)=Z$．另一方面，由于

$$1=(-2)\times4+9\in(4,9)$$

也可推得$(4,9)=Z$．故

$$(1)=(4,9)$$

7　**证**　因

$$1=\frac{1}{2}\times2+0\times x\in(2,x)$$

所以$(2,x)=F[x]=(1)$是主理想.

8 证 (1) 显然$0\in A$, 故A非空. $\forall x,y\in A, r\in R, n\in N$: 有

$$(x-y)n=xn-yn=0-0=0$$

$$(rx)n=r(xn)=r0=0$$

$$(xr)n=x(rn)=x\cdot n'=0, n'\in N$$

故$x-y$, $rx, xr\in A$, 从而A是R的理想.

(2) 证明与 (1) 类似.

§6

1 参看第一章§6.

2 参看第一章§6.

3 证 设

$$\varphi: a+bi \longrightarrow a-bi, \quad \forall a+bi\in C$$

由于每个复数都有唯一的共轭复数, 所以φ是C到C的双射, 而且$\forall \alpha=a_1+b_1i$, $\beta=a_2+b_2i\in C$有

$$\varphi(\alpha+\beta)=\varphi((a_1+a_2)+(b_1+b_2)i)=(a_1+a_2)-(b_1+b_2)i$$
$$=(a_1-bi)+(a_2-b_2i)=\varphi(\alpha)+\varphi(\beta)$$

$$\varphi(\alpha\beta)=\varphi((a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i)$$
$$=(a_1a_2-b_1b_2)-(a_1b_2+a_2b_1)i$$
$$=(a_1-b_1i)(a_2-b_2i)=\varphi(\alpha)\varphi(\beta)$$

故φ是复数域C的自同构.

4 证 假设存在

$$\varphi: Z[\sqrt{2}]\cong Z[\sqrt{3}].$$

则由命题2知

$$\varphi(1)=1$$

于是$\forall n\in Z$有

$$\varphi(n)=n$$

设 $\varphi(\sqrt{2})=x+y\sqrt{3}$，则

$$\varphi(2)=\varphi(\sqrt{2}\times\sqrt{2})=\varphi(\sqrt{2})\cdot\varphi(\sqrt{2})$$
$$=(x+y\sqrt{3})^2=x^2+3y^2+2xy\sqrt{3}$$

由前面证得的结果知 $\varphi(2)=2$。于是

$$x^2+3y^2+2xy\sqrt{3}=2, x^2+3y^2-2+2xy\sqrt{3}=0$$

此时必有

$$\begin{cases}x^2+3y^2-2=0\\xy=0\end{cases}$$

但是此方程组无整数解，这个矛盾说明不存在环 $\mathbf{Z}[\sqrt{2}]$到环 $\mathbf{Z}[\sqrt{3}]$的同构映射。

5　证　建立 R 到 R'/I' 的映射

$$\Psi:\ a\longrightarrow\overline{\varphi(a)}=\varphi(a)+I',\quad\forall a\in R$$

易证

$$\Psi:\ R\sim R'/I'$$

且 Ψ 的核 $\mathrm{Ker}\Psi=I$。由定理 1 之（2）得

$$R/I\cong R'/I'$$

6　证　$\forall f(x)\in \boldsymbol{R}[x]$，由带余除法有

$$f(x)=(x-a)q(x)+r_f,\quad r_f\in \boldsymbol{R}$$

现规定

$$\varphi:\ f(x)\longrightarrow r_f$$

易证 φ 是 $\boldsymbol{R}[x]$ 到 $\boldsymbol{R}$ 的满射，而且保持加法、乘法运算，从而

$$\varphi:\boldsymbol{R}[x]\sim\boldsymbol{R}$$

φ 的核 $\mathrm{Ker}\varphi=(x-a)$。由定理 1 之（2）得

$$\boldsymbol{R}[x]/(x-a)\cong\boldsymbol{R}$$

7　证　设 φ 是 $Q[i]$ 的任意一个自同构，则由命题 2 知

$$\varphi(0)=0,\quad\varphi(1)=1$$

进而得知 $\forall a\in Q$ 有 $\varphi(a)=a$。设 $\varphi(i)=x+yi$，则

$$\varphi(i^2)=(\varphi(i))^2=(x+yi)^2=x^2-y^2+2xyi$$

但由刚才证得的结果知

$$\varphi(i^2)=\varphi(-1)=-1$$

故

$$x^2-y^2+2xyi=-1,\ x^2-y^2+1+2xyi=0$$

此时必有

$$\begin{cases}x^2-y^2+1=0\\ xy=0\end{cases}$$

这个方程组的两组有理解是

$\begin{cases}x=0\\ y=1,\end{cases}$ $\begin{cases}x=0\\ y=-1\end{cases}$，因此$i$在$\varphi$之下的象只有两种可能：$\varphi(i)=i$或者$\varphi(i)=-i$。对$Q[i]$中任意元素 $a+bi$来说，当$\varphi(i)=i$时有

$$\varphi(a+bi)=\varphi(a)+\varphi(b)\varphi(i)=a+bi$$

当$\varphi(i)=-i$时有

$$\varphi=(a+bi)=\varphi(a)+\varphi(b)\varphi(i)=a+b(-i)=a-bi$$

从而得知，$Q[i]$的自同构共有两个

$$\varphi_1:a+bi\longrightarrow a+bi;\ \varphi_2:a+b_i\longrightarrow a-bi$$

8 证 (1) 显然$S+I$ 非空。$\forall \alpha=s_1+a_1,\beta=s_2+a_2\in S+I:s_i\in S,a_i\in I$,则因$S$，$I$是环有

$$\alpha-\beta=(s_1-s_2)+(a_1-a_2)\in S+I$$

再因I是理想而有

$$\alpha\beta=(s_1+a_1)(s_2+a_2)=s_1s_2+(s_1a_2+a_1s_2+a_1a_2)\in S+I$$

所以$S+I$是R的子环。

显然I是$S+I$的理想。

(2) 显然$S\cap I$是S的子环。$\forall a\in S\cap I,s\in S$:则由$a\in S$知$as,sa\in S$。又由$a\in I$且$I$是理想知$as,sa\in I$。故$as,sa\in S\cap I$，从而证得$S\cap I$是$S$的理想。

(3) 建立S到$S+I/I$的映射

$$\varphi:s\longmapsto\overline{s+a}=(s+a)+I=s+I=\overline{s},\quad \forall s\in S,a\in I$$

显然φ是满射，而且易证φ保持加法和乘法运算，故

$$\varphi:S\sim(S+I)/I$$

φ的核$\mathrm{Ker}\varphi=S\cap I$。由同态基本定理得

$S/S\cap I\cong (S+I)/I$

§7

1 解 (x)是 $Q[x]$ 的极大理想。

设N是 $Q[x]$ 的理想，而且 $N\supset (x)$.则在N中存在 $f(x)=a_0+a_1x+\cdots+a_nx^n$，而 $f(x)\overline{\in}(x)$。这时必有：$a_0\neq 0$。因为N是理想，所以有

$$a_0^{-1}(a_0+a_1x+\cdots+a_nx^n)=1+(a_0^{-1}a_1)x+\cdots+(a^{-1}a_n)x^n\in N$$

另一方面，因为

$$(a_0^{-1}a_1)x+\cdots+(a_0^{-1}a_n)x^n\in (x)\subset N$$

所以

$$[1+(a_0^{-1}a_1)x+\cdots+(a_0^{-1}a_n)x]-[(a_0^{-1}a_1)x+\cdots+(a_0^{-1}a_n)x^n]=1\in N$$

于是有 $N=Q[x]$。所以，(x)是 $Q[x]$的极大理想。

2 解 $(1+i)$是 $Z[i]$ 的极大理想。

只要能证明 $Z[i]/(1+i)$是域，则由本节定理1，即可知$(1+i)$是 $Z[i]$ 的极大理想。

首先，探讨一下 $Z[i]/(1+i)$的构成的情况。为此先讨论一下$(1+i)$中的元素的形式。

设 $x+y_i\in(1+i)$，则

$$x+y_i=(a+b_i)(1+i),\ a,b\in Z$$

因为

$$(a+bi)(1+i)=(a-b)+(a+b)i$$

所以有

$$x=a-b,\ y=a+b$$

$$a=\frac{x+y}{2},b=\frac{x-y}{2}$$

由上式可知，当且仅当x与y是奇偶性相同的二整数时，

则 $x+yi\in(1+i)$

而对于任二整数 x 与 y 来说，奇偶性或者相同，或者奇偶性相反。因此可知 $Z[i]/(1+i)$ 只含两个元。

而 $Z[i]/(1+i)$ 是有 1 的交换环，所以可知 $Z[i]/(1+i)$ 只能有当然理想，于是参照本章学习指导中的例题选讲之例 7，可知 $Z[i]/(1+i)$ 是域。由本节定理 1 得知 $(1+i)$ 是 $Z[i]$ 的极大理想。

3 解 因为 $p^2\in(p^2)$，而 $p\overline{\in}(p^2)$。所以 (p^2) 不是整数环 Z 的素理想。

4 解 当 $p=2$ 时，则 $(2p)=(4)$。参看本节学习指导中补充说明之 2，可知（4）是偶数环的极大理想。

设 $p\neq 2$。令 N 是偶数环 R 的理想，而且，$N\supset(2p)$。则由整数环是主理想环，可知偶数环也是主理想环，所以有：$N=(q), q\in R$。

因为 $N\supset(2p)$，所以，$2p=qt, t\in Z$，即 $q|2p$。

因为 p 是素数。所以有：$(p,q)=1$ 或 $p|q$。

但是，当 $p|q$ 时，因为，$q\in R$，有 $2|q$，而且 $(p,2)=1$，所以，$2p|q$，由此得到 $q\in(2p)$，从而有 $(q)\subseteq(2p)$。与 $N\supset(2p)$ 相矛盾。

综合上述，可知，若 $N=(q)\supset(2p)$，必有：$(p,q)=1$。

由上述知 $q|2p$，而且 $(p,q)=1$，所以有 $q|2$。而 q 是偶数，故有：$q=\pm 2$。由此可知：$(q)=R$，所以 $(2p)$ 当 $p\neq 2$ 时也是偶数环 R 的极大理想。

5 证 设 $f(x)=a_0+a_1x+\cdots+a_nx^n$，$g(x)=b_0+b_1x+\cdots+b_mx^m$

如果

$f(x)g(x)=a_0b_0+(a_1b_0+a_0b_1)x+\cdots+a_nb_mx^{n+m}\in(x)$

则必有 $a_0b_0=0$。因为 Z 是整环，所以 $a_0=0$ 或 $b_0=0$。当 $a_0=0$ 时，则 $f(x)=a_1x+\cdots+a_nx^n=(a_1+a_2x+\cdots+a_nx^{n-1})x\in(x)$；当 $b_0=0$ 时，则有 $g(x)\in(x)$。所以 (x) 是素理想。

6　证　设N为S_p的理想而且$N\supset(p)$，则在N中一定存在$\frac{a_1}{b_1}$，但$\frac{a_1}{b_1}\overline{\in}(p)$。

因为N为S_p的理想，所以 $b_1\frac{a_1}{b_1}=a_1\in N$，而且$a_1\overline{\in}(p)$，如果$a_1\in(p)$，因为$\frac{1}{b_1}\in S_p$，于是由（$p$）是$S_p$的理想，则有

$\frac{1}{b_1}a_1=\frac{a_1}{b_1}\in(p)$，与$\frac{a_1}{b_1}\overline{\in}(p)$相矛盾。

进一步，由$a_1\overline{\in}(p)$可知$p\nmid a_1$，从而$(p,a_1)=1$。

于是，在Z中存在二整数s和t使：

$$sa_1+tp=1$$

因为$a_1\in N$，$p\in(p)\subset N$，而且N是S_p的理想，所以$1\in N$。于是有$N=S_p$，即(p)是S_p的极大理想。

其次证明(p)是S_p的素理想。

设$\frac{a_1}{b_1}$，$\frac{a_2}{b_2}\in S_p$，如果$\frac{a_1}{b_1}\frac{a_2}{b_2}=\frac{a_1a_2}{b_1b_2}\in(p)$，则有$a_1a_2\in(p)$。所以在$S_p$中存在$\frac{a}{b}$，使：$a_1a_2=\frac{a}{b}p$。

因为$p\nmid b$，而p为素数，所以$(p,b)=1$。由于a_1a_2是整数，因此$\frac{ap}{b}$是整数，于是必有$b|a$，即$\frac{a}{b}$是整数。设$\frac{a}{b}=q$，则$a_1a_2=pq$，即$p|a_1a_2$。

于是由素数的性质，必有：$p|a_1$或$p|a_2$。当$p|a_1$时，则$a_1\in(p)$故有$\frac{a_1}{b_1}\in(p)$；当$p|a_2$时则有$\frac{a_2}{b_2}\in(p)$。

综合上述可知(p)是S_p的素理想。

7　证　若N是R的素理想，则对于N在R中的补集N'中的任二元素a，b，必有$ab\overline{\in}N$。否则，若$ab\in N$，由N是素理

---

* 由本节定理2直接可得（P）为素理想。

想，则 $a\in N$ 或 $b\in N$ 与$a,b\in N'$ 相矛盾．上述说明：$\forall a$、$b\in N'$有$ab\in N'$，即 N' 是乘法半群（因为环R的乘法满足结合律）．

设N'是乘法半群，去证N是环R的素理想。

若 $ab\in N$，则 a 与 b 必有其一在N中。否则，若 $a\overline{\in}N$，$b\overline{\in}N$，则 $a\in N'$，$b\in N'$。于是由 N' 是乘法半群，可知 $ab\in N'$ 即 $ab\overline{\in}N$，与 $ab\in N$相矛盾。所以，当 N' 是乘法半群时，N 是环R的素理想。

8　**解**　因为 $M_2(Q)=\left\{\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}\middle|\ a_{ij}\in Q\right\}$有真零因子，所以 $M_2(Q)$ 不能是除环。

其次证明 $M_2(Q)$ 只有平凡（当然）理想．设 $N\neq\{0\}$ 是 $M_2(Q)$的理想，只要证得$N=M_2(Q)$，则 $M_2(Q)$ 只有平凡理想即得证。

首先，容易推得，若N含$\begin{pmatrix}a&0\\0&0\end{pmatrix}$，$a\neq0$，则$N$必含 $M_2(Q)$中的单位元：$\begin{pmatrix}1&\\&1\end{pmatrix}$．因为$N$是理想．所以有 $N=M_2(Q)$．

其次说明，当环R的理想$N\neq\{0\}$时，在N中必含有元：$\begin{pmatrix}a&0\\0&0\end{pmatrix}$，$a\neq0$。

因为$N\neq\{0\}$，所以在N中存在元：$\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}\neq0$，则必有某一$a_{ij}\neq0$．而且进一步可以说明，在$N$中一定含有$a_{11}\neq0$ 的元：$\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}$。

若 $a_{12}\neq0$，则 $\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}a_{12}&a_{11}\\a_{22}&a_{21}\end{pmatrix}\in N$

若 $a_{21}\neq0$，则$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}=\begin{pmatrix}a_{21}&a_{22}\\a_{11}&a_{12}\end{pmatrix}\in N$

若 $a_{22}\neq0$，则$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}a_{22}&a_{21}\\a_{12}&a_{11}\end{pmatrix}\in N$

上述说明，在N中存在元

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, a_{11} \neq 0$$

而 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \\ 0 & 0 \end{pmatrix}$，于是由前述可知 $N = M_2(Q)$。

注：此题说明，只有平凡理想的环 R 未必一定是除环。但是，由本章学习指导的例题选讲之例 7，可以看出：如果环 R 没有真零因子时，则 R 必是除环。

§8

1　解　由商域的构成可知，$Z[i]$ 的商域为 $Q[i] = \{a + bi \mid a,\ b \in Q\}$。

2　解　$R[x]$ 的商域为 $\left\{\dfrac{f(x)}{g(x)} \middle| f(x), g(x) \in R[x], g(x) \neq 0\right\}$。

3　解　S_p 的商域 $= Q$。

4　证　设 Q 为域 F 的商域，则 $\forall x \in Q$，有 $x = \dfrac{a}{b}, a, b(\neq 0) \in F$。因为 F 是域，所以 $\dfrac{a}{b} \in Q$。由此可知。$F = Q$。

§9

1　解　（1）$fg = \overline{3}x^4 + \overline{5}x^3 + \overline{4}x,\ f - g = \overline{3}x^3 + \overline{2}x^2 + \overline{5}$；

（2）$\deg(fg) = 4$。

2　解　用反证法。若 x^k 不是 R 上的未定元，则在 R 中存在不全为 0 的元：$a_0, a_1, \cdots, a_n$，$(a_n \neq 0)$ 使：

$a_0 + a_1 x^k + \cdots + a_n (x^k)^n = 0$，从而有

$$a_0 + a_1x^k + \cdots + a_nx^{kn} = 0$$

上式说明 x 不是 R 上的未定元，与题设 x 为 R 上的未定元相矛盾。所以，x^k 是 R 上的未定元。

3 解 显然 $R[x^2]$ 是 $R[x]$ 的真子环。而

φ： $f(x) \longrightarrow f(x^2)$

是 $R[x]$ 到 $R[x^2]$ 的同构映射（验证从略）。即 $R[x] \cong R[x^2]$。

4 解 设 x 不是整环 I 的商域 Q 上的未定元，则在 Q 中存在不全为 0 的元：$\frac{a_0}{b_0}$，$\frac{a_1}{b_1}$，$\cdots$，$\frac{a_n}{b_n}$（$\neq 0$）使：$\frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x_n = 0$。其中 $a_i, b_j \in I$。$b_j \neq 0$。用 $b_0b_1\cdots b_n$ 乘上式，得到

$$(a_0b_1\cdots b_n) + (b_0a_1\cdots b_n)x + \cdots - (b_0b_1\cdots a_n)x^n = 0$$

显然 $b_0b_1\cdots a_n \neq 0$，所以 x 不是 I 上的未定元，与题设矛盾。故 x 也是 I 的商域 Q 上的未定元。

5 解 （1）因为 $R[\alpha_1,\alpha_2]$ 是由形如 $\sum a_{i_1 i_2}\alpha_1^{i_1}\alpha_2^{i_2}$ 的元组成；$R[\alpha_2, \alpha_1]$ 是由形如 $\sum a_{i_2 i_1}\alpha_2^{i_2}\alpha_1^{i_1}$ 的元组成。而 $R[\alpha_1,\alpha_2]$ 和 $R[\alpha_2\alpha_1]$ 都是交换环，所以有 $R[\alpha_1,\alpha_2] = R[\alpha_2,\alpha_1]$。

（2）设 $a_0 + a_1x_i + \cdots + a_mx_i^m = 0$ （*）

因为 $a_kx_i^k = a_kx_1^0\cdots x_{i-1}^0 x_i^k x_{i+1}^0\cdots x_n^0$，所以由 $x_1, x_2, \cdots, x_n$ 是无关未定元，（*）式成立必须 $a_k = 0$，$(k = 0, 1, \cdots, m)$。即 x_i 是 R 上的未定元。

6 解 由本节定理 3 可知。

7 $f(x_1, x_2, \cdots, x_n) \longmapsto f(y_1, y_2, \cdots, y_n)$

是 $R[x_1, x_2, \cdots, x_n]$ 到 $R[y_1, y_2, \cdots, y_n]$ 的满同态。再由 $y_1, y_2, \cdots, y_n$ 是 R 上的无关未定元，可知 η 是单射。所以 $R[x_1, x_2, \cdots, x_n] \cong R[y_1, y_2, \cdots, y_n]$。

§10

2 解 由题设 c_1 是 $f(x)$ 的 k_1 重根，所以有

$$f(x)=(x-c_1)^{k_1}q_1(x)$$

又因 c_2 是 $f(x)$ 的 k_2 重根，所以

$$f(c_2)=(c_2-c_1)^{k_1}q_1(c_2)=0$$

而 $c_1\neq c_2$，所以 $c_2-c_1\neq 0$。于是由上式有 $q_1(c_2)=0$，即 c_2 是 $q_1(x)$ 的根。由于 c_2 是 $f(x)$ 的 k_2 重根，所以进一步可知 c_2 是 $q_1(x)$ 的 k_2 重根。故有：$q_1(x)=(x-c_2)^{k_2}q_2(x)$。

于是，$f(x)=(x-c_1)^{k_1}(x-c_2)^{k_2}q_2(x)$。继续作下去，即得：$f(x)=(x-c_1)^{k_1}(x-c_2)^{k_2}\cdots(x-c_r)^{k_r}q_r(x)$。即 $(x-c_1)^{k_1}(x-c_2)^{k_2}\cdots(x-c_r)^{k_r}\mid f(x)$。

3　**解**　1 为 x^7-1 的 7 重根。

4　仿数域 F 上多项式环的证法，对多项式的次数作数学归纳法。

5　**解**　由本节定理 2 知

$$f(x)=(bx+c)q(x)+r,\ r\in I$$

故有

$$f(-b^{-1}c)=(b(-b^{-1}c)+c)q(-b^{-1}c)+r=r$$

7　**解**　经验算知 x^2+1 在 Z_3 中没有根，而 x^2+1 的次数为 2，所以 x^2+1 是 $Z[x]$ 的不可约多项式。而在 $Z_5[x]$ 中，$x^2+1=x^2-4=(x-2)(x+2)$。所以 x^2+1 是 $Z_5[x]$ 中的可约多项式。

8　**解**　因为定理 6 中的 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的公因子：$d(x)\mid f(x),g(x)$，而且

$$(d(x))=\{f(x)u(x)+g(x)v(x)\mid u(x),v(x)\in F[x]\}$$

所以有：$f(x)u_0(x)+g(x)v_0(x)=d(x)$

由上式可知，若 $d_0(x)$ 是 $f(x)$ 与 $g(x)$ 的任一公因子，则有 $d_0(x)\mid d(x)$。所以，$d(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因子。

9　**解**　若 $f(x)$ 与 $g(x)$ 中有一个是 0 多项式，不妨设 $f(x)=0$，则 $g(x)$ 即为 $f(x)$ 与 $f(x)$ 的最大公因子。若 $f(x)$ 与 $g(x)$ 都不是 0 多项式时，则 $f(x)$ 与 $g(x)$ 的任一公因子 $d(x)$ 不能是 0 多项式。由于 $\deg d(x)\leqslant\deg f(x)\ (f(x)\neq 0)$，所以在 $f(x)$ 与

$g(x)$ 的公因子中，存在次数最大的公因子，设为 $d(x)$，则由上题可知此公因子 $d(x)$ 即为 $f(x)$ 与$g(x)$ 的最大公因子。综上所述，可知对于 $F[x]$中任二多项式 $f(x)$ 和 $g(x)$，一定有最大公因子存在。至于，任意两个最大公因子只相差一个单位（可逆元）是显然的。

10　**证**　设N是$F[x]$的理想，而且$N\supset(p(x))$。因为 $F[x]$ 是主理想环，所以 $N=(q(x))$，$q(x)\in F[x]$。

由 $N\supset(p(x)$，可知 $q(x)\bar{\in}(p(x))$，于是 $p(x)\nmid q(x)$ 。由题设 $p(x)$ 是不可约多项式，所以 1 是 $p(x)$ 与 $q(x)$ 的最大公因子。于是由本节定理 6，存在 $u(x)$，$v(x)\in F[x]$ 使得：

$p(x)u(x)+q(x)v(x)=1$。

因为$(p(x))\subset N=(q(x))$，所以 $p(x)u(x)+q(x)v(x)\in N$，即$1\in N$。故有 $N=F[x]$，即 $(p(x))$是$F[x]$的极大理想。

§ 11

1　**解**　仿例 4（本节）可以证明：

（1）α 是 $Z[\sqrt{2}]$的单位（可逆元）$\Longleftrightarrow|\alpha|^2=1$；

（2）若$|\alpha|^2=25$，则 α 是 $Z[\sqrt{2}]$的素元；

（3）若 $|\alpha|^2=11$，则 α 是 $Z[\sqrt{2}]$的素元。

于是可知，$Z[\sqrt{2}]$中只有±1是单位，而 5 是素元。因 $7=(3+\sqrt{2})(3-\sqrt{2})$，$3+\sqrt{2}$ 和$3-\sqrt{2}$都是素元，而且每一个都不是 7 的相伴元，所以 7 不是素元。

2　**解**　对 $Z[i]$中的元 $\alpha=a+bi\neq0$规定：

$\delta(\alpha)=|\alpha|^2=a^2+b^2$，显然 $\delta(\alpha)$ 是非负整数。仿照本章学习指导例题选讲之例10，容易推出 $Z[i]$是欧氏环。仿例 4（本节）可以证明：

（1）α 是 $Z[i]$ 的单位（可逆元）$\Longleftrightarrow|\alpha|^2=1$，由此可知，$Z[i]$中的单位只有$\pm1$和$\pm i$。

（2）若$|\alpha|^2=5$，则 α 是 $Z[i]$ 的素元。

于是由$5=(2+i)(2-i)$可知5不是$Z[i]$的素元，而且$2+i$和$2-i$都是$Z[i]$的素元。

（3）进一步再证明$Z[i]$中适合条件：$|\alpha|^2=9$的元是素元，由此即可断定3是素元。

3 （1）$Z[\sqrt{-5}]$中的元α是单位$\Longleftrightarrow|\alpha|^2=1$。

（2）$Z[\sqrt{-5}]$中满足条件：$|\alpha|^2=9$的元α是素元。

（3）因为$9=3\cdot3=(2+\sqrt{-5})(2-\sqrt{-5})$，其中3和$2+\sqrt{-5}$，$2-\sqrt{-5}$都是素元，而且3不是$2+\sqrt{-5}$和$2-\sqrt{-5}$的相伴元。所以$Z[\sqrt{-5}]$不是唯一分解环。

4 证 设N是欧氏环R的理想，且$N\neq\{0\}$。

令 $A=\{\delta(x)\mid x\in N,x\neq0\}$,则$A$是非负整数集,而且$A\neq\phi$，于是在$A$中有最小数,设为$\delta(n_0)$，$n_0\in N$。

下面往证$N=(n_0)$。因为R是欧氏环，所以，$\forall a\in N$在R中存在q和r使：$a=n_0q+r$,其中$r=0$或$\delta(r)<\delta(n_0)$。

如果$r\neq0$。因为N是R的理想，所以$a-n_0q\in N$,即$r\in N$。于是由上述非负整数集A的定义，$\delta(r)\in A$。这与$\delta(n_0)$的最小性相矛盾。所以$r=0$。

于是，由上述可知，$\forall a\in N$ 总有$q\in R$使：

$$a=n_0q$$

即$N\subseteq(n_0)$，但$n_0\in N$，故有$N=(n_0)$。

5 **解** 设F为域。$\forall x(\neq0)\in F$ 定义$\delta(x)=n_0$。（确定的正整数）。

因为，$\forall a,b(\neq0)\in F$ 有$ab^{-1}\in F$，即在F中有q使得：$ab^{-1}=q$,即$a=bq$.所以F是欧氏环。

6 证 若a与b都为0时，则a与b的最大公因子是0。所以有

$$a\cdot0+b\cdot0=0$$

下面对a与b不全为0的情形证明命题成立。

令(a,b)是a和b所生成的理想（I的）。则因I是主理想环，所以有：$(a,b)=(d_0)$，$d_0\in I$.显然$d_0\neq0$.于是有u_0,v_0

$\in I$ 使得

$$d_0=au_0+bv_0 \qquad (*)$$

设 d 是 a 与 b 的最大公因子，因 a 与 b 不全为 0，所以 $d\neq 0$，而且 $d|a,b$。于是由（*）式可知：$d|d_0$。

另一方面，因 $(d_0)=(a,b)$，所以有

$$a=d_0a_1,\quad b=d_0b_1,\quad a_1,b_1\in I$$

即 d_0 是 a 与 b 的公因子。而 d 是 a 与 b 的最大公因子，所以 $d_0|d$。故有 $d_0=d\varepsilon$，ε 是 I 的单位。于是由（*）式有

$$au_0+bv_0=d\varepsilon$$

从而有

$$au_0\varepsilon^{-1}+bv_0\varepsilon^{-1}=d$$

取 $u=u_0\varepsilon^{-1}$，$v=v_0\varepsilon^{-1}$，则有 $au+bv=d$。

7 证 首先，由 S_p 的性质可知，S_p 的元 $\frac{a}{b}$ 是 S_p 的单位（可逆元）$\Longleftrightarrow p\nmid a$。

其次，设 $N\neq\{0\}$ 是 S_p 的理想，如果在 N 中存在 S_p 的单位 ε 时，则 $\varepsilon^{-1}\varepsilon=1\in N$。于是 $N=(1)$。

若 N 中的任意元 $\frac{a}{b}$ 都不是 S_p 的单位（可逆元），则 $p|a$，$\forall\frac{a}{b}\in N$。于是有 $\frac{a}{b}=p^{*}\frac{a_1}{b}$，$p\nmid a_1$，

由上述可知，当理想 N 的每个元都不是 S_p 的单位（可逆元）时，则 $N\subseteq(p)$。显然 N 是 (p) 的理想，所以由 (p) 的构成可知 N 是主理想。于是知 S_p 是主理想环，所以 I 是唯一分解环。

8 证 设 $f(x)=a_0+a_1x+\cdots+a_nx^n$

$$g(x)=b_0+b_1x+\cdots+b_mx^m$$

是两个本原多项式，去证 $f(x)g(x)$ 也是本原多项式。

假定 $f(x)g(x)$ 不是本原多项式，设

$$f(x)g(x)=c_0+c_1x+\cdots+c_{n+m}x^{n+m}$$

则 $c_0, c_1, \cdots, c_{n+m}$ 的最大公因子不是单位（可逆元），因为 I 是唯一分解环，所以存在素元 $p \in I$，使得：$p | c_i$，$i = 0, 1, \cdots, n+m$。

但因 $f(x)$ 和 $g(x)$ 都是本原多项式，所以 p 不能整除所有 a_i，也不能整除所有 b_i。

设 a_r 是 a_i 中不能被 p 整除的足码最小者，即 $p | a_0, \cdots, a_{r-1}$，但 $p \nmid a_r$。再设 b_i 中不能被 p 整除的足码最小的是 b_s，即 $p | b_0, b_1, \cdots, b_{s-1}$，但 $p \nmid b_s$。但是

$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0$，而 c_{r+s}，$a_0, a_1, \cdots, a_{r-1}, b_{s-1}, \cdots, b_1, b_0$ 都能被 p 整除，所以 $p | a_r b_s$。因 I 是唯一分解环，所以由本节定理1的推论知，$p | a_r$ 或 $p | b_s$。与 $p \nmid a_r$ 和 $p \nmid b_s$ 相矛盾，所以 $f(x)g(x)$ 是本原多项式。

第四章　模习题解答

§1

2. 证　$\forall x, y \in M, a, b \in R$　有：

（1）$(x+y)\cdot a = a(x+y) = ax + ay = x\cdot a + y\cdot a$

（2）$x\cdot(a+b) = (a+b)x = ax + bx = x\cdot a + x\cdot b$

（3）$x\cdot(ab) = (ab)x = (ba)x = b(ax) = b(x\cdot a)$

$$= (x\cdot a)\cdot b$$

于是加群M关于运算“·”构成交换环R上的右模。

3. 证　由于R是非交换的，则存在$a, b \in R$，使$ab \neq ba$，对$x \in M$，$x \neq \theta$考察

$$x\cdot(ab) = (ab)x$$

而

$$(x\cdot a)\cdot b = (ax)\cdot b = b(ax) = (ba)x$$

如果M关于“·”构成R上的右模，则

$$x\cdot(ab) = (x\cdot a)\cdot b$$

于是推得

$$(ab - ba)x = \theta$$

由于R是除环，$ab - ba \neq 0$，知$(ab-ba)^{-1}$存在，又由R是除环知$1x = \theta$，与M是单式模矛盾。故M关于运算“·”不能构成环R上右模。

4 证　$\forall x, y \in M$，$a, b \in R$，有

（1）$(x+y)\cdot a = \varphi(a)(x+y) = \varphi(a)x + \varphi(a)y$

$$= x\cdot a + y\cdot a$$

（2） $x\cdot(a+b)=\varphi(a+b)x=\varphi(a)x+\varphi(b)x$

$$=x\cdot a+x\cdot b$$

（3） $x\cdot(ab)=\varphi(ab)x=[\varphi(b)\varphi(a)]x=\varphi(b)[\varphi(a)x]$

$$=\varphi(b)[x\cdot a]=[x\cdot a]\cdot b$$

于是M关于运算“·”构成环R上的右模。

5 证 $\forall x,y\in M,a,b\in S$有

（1） $a\cdot(x+y)=\varphi(a)(x+y)=\varphi(a)x+\varphi(a)y$

$$=a\cdot x+a\cdot y$$

（2） $(a+b)\cdot x=\varphi(a+b)x=[\varphi(a)+\varphi(b)]x$

$$=\varphi(a)x+\varphi(b)x=a\cdot x+b\cdot x$$

（3） $(ab)\cdot x=\varphi(ab)x=[\varphi(a)\varphi(b)]x$

$$=\varphi(a)[\varphi(b)x]=a\cdot(b\cdot x)$$

于是M关于运算“·”构成S上的左模。

6 证 设M是加群，已知关于运算

$$nx=\begin{cases}\overbrace{x+x+\cdots+x}^{n} & n>0\\ 0 & n=0\\ \overbrace{(-x)+(-x)+\cdots+(-x)}^{n} & n<0\end{cases}$$

构成Z—模。如果还存在运算“·”，使M在“·”下构成Z—模。那么，当$n>0$时，有

$$n\cdot x=\overbrace{(1+1+\cdots+1)}^{n}\cdot x$$

$$=1\cdot x+1\cdot x+\cdots+1\cdot x=x+x+\cdots+x=nx$$

当$n<0$时，有$n=-m$，$m>0$，于是

$$n\cdot x=(-m)\cdot x=-(m\cdot x)=-(mx)=(-m)x$$

$$=nx$$

当$n=0$时，显然有

$$n\cdot x=0\cdot x=\theta=0x=nx$$

所以倍乘运算是唯一的。

7 证 如果存在倍乘运算“∘”使M在Q上成单式模。

那么对$n\in Z\subset Q$，据6题有

$$n\circ x=nx=n\cdot x,\quad \forall x\in M$$

而对$\frac{1}{n}\in Q\ (n\neq 0)$，则有

$$n\circ\left(\frac{1}{n}\cdot x\right)=n\cdot\left(\frac{1}{n}\cdot x\right)=\left(n\frac{1}{n}\right)\cdot x$$

$$=1\cdot x=1\circ x=\left(n\frac{1}{n}\right)\circ x$$

$$=n\circ\left(\frac{1}{n}\circ x\right)$$

由$n\subset Q$，Q是域，于是得到

$$\frac{1}{n}\circ x=\frac{1}{n}\cdot x$$

对任意 $a=\frac{n}{m}\in Q\ (m,n\in Z，m\neq 0)$，有

$$a\circ x=\frac{n}{m}\circ x=\left(n\frac{1}{m}\right)\circ x$$

$$=n\circ\left(\frac{1}{m}\circ x\right)=n\cdot\left(\frac{1}{m}\cdot x\right)$$

$$=\left(n\frac{1}{m}\right)\cdot x=a\cdot x$$

从而知运算“$\circ$”与运算“$\cdot$”是相等的，M在Z上成单式模的倍乘运算只能是唯一的．

8 **解** 不能．否则，若M在倍乘“$\cdot$”下，构成Q上的单式模，那么，取$x\in M,x\neq\theta$，由M的有限性，知x的阶数n是有限的非负整数，据7题有

$$n\cdot x=nx=\theta$$

于是

$$x=1\cdot x=\left(\frac{1}{n}\cdot n\right)\cdot x=\frac{1}{n}\cdot(n\cdot x)$$

$$= \frac{1}{n} \cdot \theta = \theta$$

矛盾。

§2

1 证 (3) $\forall\ x = \sum_{i=1}^{n} a_i x_i \in M$，有

$$x = \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} (a_i \cdot 1) x_i = \sum_{i=1}^{n} a_i (1 x_i)$$

$1 x_i \in N$，$i = 1, 2, \cdots, n$。于是知N是M的一个生成集。

2 解 用“·”记倍乘的形式乘法，有

$M_1 = \{a \cdot 2 \mid a \in \mathbf{Z}\}$

$M_2 = \{b \cdot 3 \mid b \in \mathbf{Z}\}$

$M_3 = \{a \cdot 2 + b \cdot 3 \mid a, b \in \mathbf{Z}\}$

当$1 \cdot 2 = 2$，$1 \cdot 3 = 3$时，有

$M_1 = (2)$，$M_2 = (3)$，$M_3 = \mathbf{Z}$

3 证 $\forall x \in \mathbf{Z}$，对于$y \in \mathbf{Z}$，都存在零次多项式$f(\lambda) = x \in \mathbf{Z}[\lambda]$，使

$x = f(\lambda) \cdot y = f(y)$

于是知：$\mathbf{Z} = L(y)$。

4 解 $S = \{ax + by \mid a, b \in R\}$

$S^{(2)} = \{(a_1 x + b_1 y,\ a_2 x + b_2 y) \mid a_1, b_1, a_2, b_2 \in R\}$

于是知$S^{(2)}$在R上的生成集为：

$\{(x, 0), (y, 0), (0, x), (0, y)\}$

5 解 设S是R－模M的一个有限生成集。如果S不是最小生成集，则必含有真子集S_1，使S_1也是生成集；如果S_1仍不是最小的，则S_1必含有真子集S_2，S_2是模M在R上的生成集；如此下去，得出模M在R上的生成集序列

$S \supset S_1 \supset S_2 \supset \cdots$

由S是有限的，可知序列的长也是有限的。

$$S\supset S_1\supset\cdots\supset S_k$$

S_k就是最小生成集。

§3

1　解　不一定。当R是除环时则一定能。

2　证　反证。如果$U=\{u_i\}_{i=1}^{n}$不是R－模M的最小生成集。则必存在U的真子集V，使V是M在R上的生成集，不妨设$V=\{u_i\}_{i=1}^{n-1}$，于是存在$a_i\in R$，$i=1,2,\cdots,n-1$，使 $u_n=\sum_{i=1}^{n-1}a_iu_i$，从而有

$$a_1u_1+a_2u_2+\cdots+a_{n-1}u_{n-1}+(-1)u_n=\theta$$

U是一个线性相关组，这与U是自由基矛盾。

3　证　（1）当$i=1$时，$\forall x=au_1$，$y=bu_1\in Ru_1$，有$x+y=(a+b)u_1\in Ru_1$，于是知：Ru_1是加群；$\forall r\in R$，$x=au_1\in Ru_1$，有

$$rx=r(au_1)=(ra)u_1\in Ru_1$$

不难验证：Ru_1是R上的模

$$u_1=1u_1\in Ru_1$$

且$\forall x\in Ru_1$都可表为$x=au_1$，$a\in R$的形式，于是知u_1是Ru_1在R上的一个生成集。又当$au_1=\theta$时，则有

$$au_1+0u_2+\cdots+0u_n=\theta$$

由于U是线性无关的，故 $a=0$，于是知u_1在R上是线性无关的，从而得知：Ru_1是自由模。$U_1=\{u_1\}$是Ru_1的R—自由基，秩数是1。

（2）取$W=\{e_i\}_{i=1}^{n}$　$e_i=(\overbrace{0\cdots0\ 1}^{i}\ 0\cdots0)$，$i=1,2,\cdots,n$则有

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} & a_{22} \cdots a_{2n} \\ \cdot & \cdot \cdots \cdot \\ a_{n1} & a_{n2} \cdots a_{nn} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}$$

由U是$R^{(n)}$的一个自由基，可知$A=(a_{ij})$是可逆阵，于是存在$B=(b_{ij})$，$b_{ij}\in R$，使$AB=E$于是得：

$$a_{11}b_{11}+a_{12}b_{21}+\cdots+a_{1n}b_{n1}=1$$

如果a_{1j}都是非单位，则$1=\sum\limits_{j=1}^{n}a_{1j}b_{j1}\in N$，这与$N$是真理想矛盾。故$a_{1j}$中至少有1个是单位。

（3）由$a_{1j}(j=1,2,\cdots,n)$中至少有一个是单位，故由$a_{11},a_{12},\cdots,a_{1n}$生成的理想

$$\langle a_{11},a_{12},\cdots,a_{1n}\rangle=R$$

（4）不妨设a_{1j_0}是单位，N是真理想，则$a_{1j}\overline{\in}N$，于是$\overline{a}_{1j}\neq\overline{0}$，由$N$含有所有非单位，知$N$是极大理想，故$R/N$是域，从而非零的$\overline{a}_{1j}$是可逆元。

4　解（1）是。因为如果$X=\{x_i\}_{i=1}^{n}$是R上的线性无关组，则对任一组不全为零$a_i\in R,(i=1,2,\cdots,n)$皆有

$$\sum_{i=1}^{n}a_ix_i\neq\theta$$

由$Z\subset R$，知对任一组Z中不全为零的标量$b_i(i=1,2,\cdots,n)$，必是R中的标量组，故有

$$\sum_{i=1}^{n}b_ix\neq\theta$$

于是断定X是Z上的线性无关组。

（2）不是。如对$x_1=(1\ 0\cdots 0)$，$x_2=(i\ 0\cdots 0)\in R^{(n)}$，有$1,i\in R$，使

$$1x_1+ix_2=\theta$$

故$\{x_1,x_2\}$是R上的线性相关组，而$\forall a,b\in Z$，若

$$ax_1 + bx_2 = (a + bi\ 0 \cdots 0) = \theta$$

则有

$$a + bi = 0$$

故$a = 0$，$b = 0$，于是知$\{x_1, x_2\}$是Z上线性无关组。

（3）是自由的，秩数是$2n$。因为对

$$x = (a_1 + b_1 i,\ a_2 + b_2 i + \cdots + a_n + b_n i) \in M$$

则有

$$x = \sum_{j=1}^{n} a_j e_j + \sum_{j=1}^{n} b_j (ie_j)$$

$$e_j = (\overbrace{0, \cdots, 0, 1}^{j}, 0, \cdots, 0)$$

于是知

$$\{e_j\}_{j=1}^{n} \cup \{ie_j\}_{j=1}^{n}$$

是$R^{(n)}$在Z上的生成集，且若

$$\sum_{j=1}^{n} a_j e_j + \sum_{j=1}^{n} b_j (ie_j) = \theta$$

则有

$$(a_1 + b_1 i,\ a_2 + b_2 i + \cdots + a_n + b_n i) = \theta$$

故得　$a_j + b_j i = 0 (j = 1, 2, \cdots, n)$。　于是断定：$a_j = 0, b_j = 0$，$(j = 1, 2, \cdots, n)$。从而知

$$\{e_j\}_{j=1}^{n} \cup \{ie_j\}_{j=1}^{n}$$

是$R^{(n)}$在Z上的自由基。Z—自由模$R^{(n)}$的秩数为$2n$。

5　证（1）设 $U = \{u_i\}_{i=1}^{n_1}$ 是模 M_1 的 R—自由基，$V = \{v_j\}_{j=1}^{n_2}$是M_2在R上的自由基，由此得 R—模M的两个子集

$$U' = \{(u_i 0) \mid u_i \in U\}$$

$$V' = \{(0\ v_j) \mid v_j \in V\}$$

对　$x = (x_1, x_2) \in M$，则有$x_1 \in M_1$，$x_2 \in M_2$，于是有

$$x_1 = \sum_{i=1}^{n_1} a_i u_i,\quad x_2 = \sum_{j=1}^{n_2} b_j v_j$$

从而得

$$x=\left(\sum_{i=1}^{n_1}a_iu_i,\ \sum_{j=1}^{n_2}b_jv_j\right)$$

$$=\left(\sum_{i=1}^{n_1}a_iu_i\quad 0\right)+\left(0\quad \sum_{j=1}^{n_2}b_jv_j\right)$$

$$=\sum_{i=1}^{n_1}a_i(u_i\quad 0)+\sum_{j=1}^{n_2}b_j(0\quad v_j)$$

故知　$U'\cup V'$ 是M在R上的一个生成集。又若

$$\sum_{i=1}^{n_1}a_i(u_i\quad 0)+\sum_{j=1}^{n_2}b_j(0\quad v_j)=\theta$$

则有

$$\left(\sum_{i=1}^{n_1}a_iu_i\quad 0\right)+\left(0\quad \sum_{j=1}^{n_2}b_jv_j\right)=\theta$$

$$\left(\sum_{i=1}^{n_1}a_iu_i\ \sum_{j=1}^{n_2}b_jv_j\right)=\theta$$

于是得

$$\sum_{i=1}^{n}a_iu_i=\theta\in M_1,\quad \sum_{j=1}^{n}b_jv_j=\theta\in M_2$$

故知　$a_i=0$，$b_j=0$($i=1,2,\cdots,n_1$;　$j=1,2,\cdots,n_2$)。从而断定$U'\cup V'$ 是M的R—自由基。M是R上的 n_1+n_2 秩自由模。

6　**解**　若M是R上的自由模，则M不一定是Q上的模。如　$Q=M_2(Z)$，则

$$R=\left\{\begin{pmatrix}a&0\\0&a\end{pmatrix}\middle|\ \forall a\in Z\right\}$$

是Q的子环。取$M=(R,+)$,则M是R—模，但M不是Q—模，因为如取标量

$$\begin{pmatrix}1&1\\0&0\end{pmatrix}\in Q$$

及模元素

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\in M$$

则有

$$\begin{pmatrix}1&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\begin{pmatrix}1&1\\0&0\end{pmatrix}\overline{\in}M$$

倍乘不封闭，M不是Q—模。

如果R是Q的理想，则M是Q上的模。事实上。令：$U=\{u_i\}_{i=1}^n$是M的R—自由基，则

$$M=\left\{\sum_{i=1}^n a_i u_i \mid a_i\in R\right\}$$

此时，对 $q\in Q$，$x=\sum_{i=1}^n a_i u\in M$，则有

$$qx=q\sum_{i=1}^n a_i u_i=\sum_{i=1}^n (qa_i)u_i$$

由于R是Q的理想，可知$qa_i\in R(i=1,2,\cdots,n)$，于是知$qx\in M$ $\forall q\in Q$，$x\in M$ 都成立。以此来定义Q乘M的倍乘运算，易证M是Q—模。

§ 4

1 解 Z_6—自由基只有两个：$U=\{\overline{1}\}$，$V=\{\overline{5}\}$。U到V的演化阵$A=\overline{5}$．V到U的演化阵为$A^{-1}=\overline{5}$。$[\overline{3}]_U=\overline{3}$，$[\overline{3}]_V=\overline{3}$，$[\overline{2}]_U=\overline{2}$，$[\overline{2}]_V=\overline{4}$。

3 证 已知$\{e_i=(0\cdots0\overset{i}{1}0\cdots0)\}_{i=1}^n$是模$Z^{(n)}$的一个$Z$—自由基，且有

$$\begin{pmatrix}u_1\\u_2\\\vdots\\u_n\end{pmatrix}=A\begin{pmatrix}e_1\\e_2\\\vdots\\e_n\end{pmatrix}$$

于是知：U是$Z^{(n)}$的Z—自由基$\Longleftrightarrow A$ 在Z上可逆$\Longleftrightarrow \det A = \pm 1$。

4　**提示**　（1）先找出一个自由基U，再在R上作一个可逆阵C，用C去演化U可得到另一个R—自由基V。

（2）因为

$$\mathrm{Mat}_U(f(\varphi, \psi)) = \mathrm{Mat}_U I_M + \mathrm{Mat}_U \varphi + \mathrm{Mat}_U(\psi) + \mathrm{Mat}_U(\varphi\psi)$$

这里

$$\mathrm{Mat}_U I_M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\mathrm{Mat}_U(\varphi) = \begin{pmatrix} 1 & 0 & i \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\mathrm{Mat}_U(\psi) = C^{-1}\begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{pmatrix} C$$

$$\mathrm{Mat}_U(\varphi\psi) = \mathrm{Mat}_U(\psi)\mathrm{Mat}_U(\varphi)$$

将这些都求出，再代入 $\mathrm{Mat}_U(f(\varphi, \psi))$中即可。

6　**解**　（1）设$U = \{u_i\}_{i=1}^n$是模M的R—自由基，令　$\varphi_{ij} \in \mathrm{End}_R(M)$，而且有

$$\mathrm{Mat}_U(\varphi_{ij}) = \begin{pmatrix} 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \begin{matrix} \\ \\ \\ (i) \\ \\ \\ \\ \end{matrix} = E_{ij},$$

$$\qquad\qquad (j)$$

则

$$\Phi=\{\varphi_{ij}\in \mathrm{End}_R(M)\mid i,j=1,\ 2,\ \cdots,n\}$$

是模$\mathrm{End}_R(M)$的R—自由基，事实上，对于

$$\forall\varphi\in \mathrm{End}_R(M)$$

有

$$\mathrm{Mat}_U(\varphi)=A=(a_{ij})=\sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}a_{ij}E_{ij}$$

$$=\sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}a_{ij}\mathrm{Mat}_U(\varphi_{ij})$$

于是

$$\varphi=\sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}a_{ij}\varphi_{ij}\quad,\ a_{ij}\in R$$

而且当

$$\sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}a_{ij}\varphi_{ij}=0\ （变换）$$

时，则有

$$\sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}a_{ij}\mathrm{Mat}_U\varphi_{ij}=\mathrm{Mat}_U0$$

于是

$$\begin{pmatrix}a_{11} & a_{12}\cdots a_{1n}\\ a_{21} & a_{22}\cdots a_{2n}\\ & \cdots \\ a_{n1} & a_{n2}\cdots a_{nn}\end{pmatrix}=\begin{pmatrix}0 & 0\cdots 0\\ 0 & 0\cdots 0\\ \cdot & \cdots\cdot\\ 0 & 0\cdots 0\end{pmatrix}$$

故$a_{ij}=0\quad(i,\ j=1,\ 2,\ \cdots,\ n)$，从而断言：$\Phi$是模$\mathrm{End}_R(M)$的一个$R$—自由基，$\mathrm{End}_R(M)$是$R$上$n^2$秩自由模。

§5

1 证由$\{x_i\}_{i=1}^{m+1}$是线性相关的，可知存在$a_1,a_2,\ \cdots,\ a_m,\ a_{m+1}\in K$，不全为零，使

$$\sum_{i=1}^{m+1} a_i x_i = \theta$$

于是可断定 $a_{m+1} \neq 0$，否则将有

$$\sum_{i=1}^{m} a_i x_i = \theta$$

此时由于$\{x_i\}_{i=1}^{m}$是线性无关的，将有$a_i = 0$，$i = 1, 2, \cdots, m$，这与a_1，a_2，…，a_m，a_{m+1}不全为零矛盾，于是得

$$x_{m+1} = \sum_{i=1}^{m} (-a_{m+1}^{-1}) a_i x_i$$

2　证　设x_1，x_2，…，x_m是线性相关的，去证x_1'，x_2'，…，x_m'也线性相关。反证：如果x_1'，x_2'，…，x_m'线性无关，考查向量组x_1，x_2，…，x_m。当

$$\sum_{i=1}^{m} a_i x_i = \theta$$

时，有

$$\sum_{i=1}^{m} a_i x_i = \sum_{i=1}^{m-1} a_i x_i' + a_m (x_m' - b x_1)$$

$$= (a_1 - a_m b) x_1' + \sum_{i=2}^{m} a_i x_i' = \theta$$

于是　$a_1 - a_m b = 0, a_i = 0$　$(i = 2, \cdots, m)$，由$a_m = 0$，易知$a_1 = 0$，故x_1，x_2，…，x_m线性无关。矛盾。

再设x_1'，x_2'，…，x_m'线性相关，往证　x_1，x_2，…，x_m也线性相关。反证：如果x_1，x_2，…，x_m线性无关，考查向量组x_1'，x_2'，…，x_m'，当

$$\sum_{i=1}^{m} a_i x_i' = \theta$$

时，有

$$\sum_{i=1}^{m} a_i x_i' = \sum_{i=1}^{m-1} a_i x_i + a_m (x_m + b x_1)$$

$$= (a_1 + a_m b) x_1 + \sum_{i=2}^{m} a_i x_i = \theta$$

于是得

$$\left.\begin{array}{r} a_1 + a_i b = 0 \\ a_i = 0 \end{array}\right\}$$

$i = 2, 3, \cdots, m$，解得： $a_1 = a_2 = \cdots = a_m = 0$，故$x'_1$，$x'_2$，$\cdots$，$x'_m$是线性无关的，矛盾。

3 证 据 2 题可知：x_1，x_2，$\cdots$，x_m 线性无关，必要且只要x_1，x'_2，x_3，$\cdots$，x_m线性无关；而 x_1，x'_2，x_3，$\cdots$，x_m线性无关必要且只要x_1，x'_2，x'_3，x_4，$\cdots x_m$ 线性无关。$\cdots$，$\cdots$如此下去，最后得：x_1，$x'_2 \cdots$，x'_{m-1}，x_m 线性无关必要且只要 x_1，x'_2，$\cdots$，x'_{m-1}，x'_m 线性无关。从而得知：x_1，x_2，$\cdots$，x^m 线性无关必要且只要x'_1，x'_2，$\cdots$，x'_m线性无关。

4 证 设 x_1，x_2，$\cdots$，x_{n+1} 是K上 n 维向量空间 V 的 $n+1$个向量，不妨设 $x_1 \neq \theta$，令 $U = \{e_i\}_{i=1}^n$ 是V的一个K—基，对 n 进行归纳：

当$n = 1$时，有 $x_1 = a_1 e_1$，$x_2 = a_2 e_1$，由于$x_1 \neq \theta$，知$a_1 \neq 0$，于是有$e_1 = a_1^{-1} x_1$，从而得：

$$x_2 = (a_2 \ a_1^{-1}) x_1$$

x_1，x_2是线性相关组，命题成立。

假如$n-1(n>1)$时命题成立。那么若

$$x_1 = a_{11}e_1 + a_{12}e_2 + \cdots + a_{1n}e_n$$

$$x_2 = a_{21}e_1 + a_{22}e_2 + \cdots + a_{2n}e_n$$

$$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$$

$$x_{n+1} = a_{n+1\,1}e_1 + a_{n+1\,2}e_2 + \cdots + a_{n+1\,n}e_n$$

是线性无关的，由 $x_1 \neq \theta$，知a_{1j} 不能全是零，不妨设$a_{1n} \neq 0$，于是得向量组

$$x'_1 = x_1$$

$$x'_j = x_j - a_{jn} a_{1n}^{-1} x_1 \qquad j = 2, 3, \cdots, n+1$$

也是线性无关的，但由于

$$x'_j = \sum_{i=1}^{n} a_{ji} e_i - a_{jn} a_{1n}^{-1} \left(\sum_{i=1}^{n} a_{1i} e_i \right)$$

$$= \sum_{i=1}^{n-1} (a_{ji} - a_{jn} a_{1n}^{-1} a_{1i}) e_i$$

于是可知，$x_j'(j=2, 3, \cdots, n+1)$ 这 n 个向量都属于除环 K 上以 $U=\{e_i\}_{i=1}^{n-1}$ 为 K—基的 $n-1$ 维向量空间 V'，据归纳假设，$\{x_j'\}_{j=2}^{n+1}$ 这 n 个向量一定是线性相关的，从而可知：x_1'，x_2'，$\cdots$，x_{n+1}' 也是线性相关的。于是断言：x_1，x_2，$\cdots$，x_{n+1} 也是线性相关的。

5　证　如果　向量组　x_1、x_2，$\cdots$，x_m 是线性相关的，那么在 K 中存在不全为 0 的 b_1，b_2，$\cdots$，b_m，使

$$\sum_{i=1}^{m} b_i x_i = \theta$$

于是有

$$\sum_{i=1}^{m} b_i x_i = \sum_{i=1}^{m} b_i \left(\sum_{j=1}^{n} a_{ij} e_j \right)$$

$$= \sum_{j=1}^{n} \left(\sum_{i=1}^{m} b_i a_{ij} \right) e_j = \theta$$

故得

$$\sum_{i=1}^{m} b_i a_{ij} = 0, \quad j=1, 2, \cdots, n$$

从而知 $(b_1, b_2, \cdots, b_n)$ 是 K 上方程组

$$\sum_{i=1}^{m} \xi_i a_{ij} = 0 \quad j=1, 2, \cdots, n$$

的非零解；反之，若方程组

$$\sum_{i=0}^{m} \xi_i a_{ij} = 0 \quad j=1, 2, \cdots, n$$

在 K 上有非零解 $(b_1, b_2, \cdots, b_n)$，则有

$$\sum_{i=1}^{m} b_i a_{ij} = 0$$

于是

$$\theta=\sum_{j=1}^{n}\left(\sum_{i=1}^{m} b_i a_{ij}\right) e_j=\sum_{i=1}^{m} b_i\left(\sum_{j=1}^{n} a_{ij} e_j\right)$$

$$=\sum_{i=1}^{m} b_i x_i$$

从而知：x_1，x_2，…，x_m是V的一个线性相关组。

6 **解** 在K上n维向量空间V中，考查向量组

$$x_i=\sum_{j=1}^{n} a_{ij} e_j, \quad i=1, 2, \cdots, m$$

由$m>n$知道这是K上线性相关组，于是存在不全为零的b_1，b_2，…，$b_m \in K$，使

$$\sum_{i=1}^{m} b_i x_i=\theta$$

从而有

$$\sum_{i=1}^{m} b_i\left(\sum_{j=1}^{n} a_{ij} e_j\right)=\sum_{j=1}^{n}\left(\sum_{i=1}^{m} b_i a_{ij}\right) e_j=\theta$$

故得

$$\sum_{i=1}^{m} b_i a_{ij}=0, \quad j=1, 2, \cdots, n$$

即线性方程组

$$\sum_{i=1}^{m} \xi_i a_{ij}=0, \quad j=1, 2, \cdots, n$$

在K上存在非零解$(b_1, b_2, \cdots, b_m)$

7 **解** 在V的向量组

$$\{f_1, f_2, \cdots, f_r, e_1, e_2, \cdots, e_n\}$$

中，（不妨设$r<n$），e_1，e_2，…e_n部分至少有一个e_{i_1}不能被f_1，f_2，…，f_r线性表出。（否则都能被f_1，f_2，…，f_r线性表出则$F=\{f_i\}_{i=1}^{r}$是V的K—基，矛盾）于是得出一个线性无关部分组

$$\{f_1, f_2, \cdots, f_r, e_{i_1}\}$$

当$r+1<n$时，可在其余的e_j $j=1$，…，i_1-1，i_1+1，…，n

中选出e_{i_2}，不能被$f_1, f_2, \cdots, f_r, e_{i_1}$线性表出，…如此下去，可在

$$\{f_1, f_2, \cdots, f_r, e_1, e_2, \cdots, e_n\}$$

中选出一个“极大”线性无关组

$$\{f_1, f_2, \cdots, f_r, e_{i_1}, e_{i_2}, \cdots, e_{i_h}\}$$

$r+h=n$，进而可断言它是一个K—基

9　证（1）$\forall x, y \in BM$，则

$$x=\sum_{i=1}^{m} a_i x_i \quad a_i \in B, \ x_i \in M$$

$$y=\sum_{j=1}^{n} b_j y_j, \quad b_j \in B, \ y_j \in M$$

于是得

$$x-y=\sum_{i=1}^{m} a_i x_i-\sum_{j=1}^{n} b_j y_j=\sum_{k=1}^{m+n} c_k z_k$$

其中

$$c_k=\begin{cases} a_i & k=i \quad j=1, 2, \cdots, m \\ -b_j & k=m+j \quad j=1, 2, \cdots, n \end{cases}$$

$$z_k=\begin{cases} x_i & k=i \quad i=1, 2, \cdots, m \\ y_j & k=m+j \quad j=1, 2, \cdots, n \end{cases}$$

所以$c_k \in B$，$z_k \in M$故$x-y \in BM$，BM是M的子群。

（2）易证加群M/BM是R/B上的模．进而欲证是向量空间，只要证此模是除环R/B上的有限生成模就可以了．设$U=\{u_i\}_{i=1}^{n}$是R—模M的有限生成集，则M/BM中有限集$\overline{U}=\{\overline{u}_i=u_i+BM\}_{i=1}^{n}$也是模$M/BM$的一个生成集．事实上，$\forall \overline{x} \in M/BM$有

$$\overline{x}=x+BM=\sum_{i=1}^{n}(a_i u_i+BM)$$

$$=\sum_{i=1}^{n} \overline{a_i u_i}=\sum_{i=1}^{n} \overline{a}_i \overline{u}_i$$

因此知：$\overline{U}$是M/BM在R/B上的有限生成集．故模 M/BM 是除环R/B上向量空间。

（3）设$U=\{u_i\}_{i=1}^n$是模 M 在R上的最小生成集．则$\overline{U}=\{\overline{u}_i\}_{i=1}^n$也是模$M/BM$在$R/B$上的最小生成集．否则必有一个$\overline{u}_i$，$1\leq i\leq n$，能被其余向量线性表出，不妨设为$\overline{u}_n$，于是有

$$\overline{u}_n=\sum_{i=1}^{n-1}\overline{a}_i\overline{u}_i$$

$$u_n+BM=\sum_{i=1}^{n-1}(a_i+B)(u_i+BM)$$

于是得

$$u_n=\sum_{i=1}^{n-1}a_iu_i+\omega,\ \omega\in BM$$

其中ω可表为$\sum_{i=1}^{n}b_iu_i$　$b_i\in B$，从而得

$$(1-b_n)u_n=\sum_{i=1}^{n-1}(a_i+b_i)u_i$$

$1-b_n\in B$，在R中可逆．于是得

$$u_n=\sum_{i=1}^{n-1}(1-b_n)^{-1}(a_i+b_i)u_i$$

这与U是模M的最小生成集矛盾．故$\overline{U}$是向量空间M/BM的R/B—基。

§6

1　**解**　设L是K上n维向量空间V的一维子空间，则存在L的K—基$\{x\}$，使

$$L=Kx=\{kx\mid k\in K\}$$

如果N是L的子模，且$N\neq\{\theta\}$，则有$y\in N$，$y\neq\theta$由$y\in L$可

知：$y=ax$，$a\in K, a\neq 0$，于是得：$x=a^{-1}y\in N$，故$L=N$。从而断言：L没有真子模，是K上的单模。

在一般环上，结论不一定成立，如考察Z一模$Z^{(2)}$，取$x=(1,0)\in Z^{(2)}$，在Z上生成1秩自由子模：

$$L=\{ax|a\in Z\}=\{(a\quad 0)|a\in Z\}$$

再取$y=(2\quad 0)\in Z^{(2)}$，在Z上生成1秩自由子模

$$N=\{by|b\in Z\}=\{(2a,\ 0)|a\in Z\}$$

此时 $N\subset L$，L不是单模。

2　证　设$L(x)$，$L(y)$是除环K上n维向量空间中二个一维子空间，且$L(x)\neq L(y)$。于是可知x和y是K上的线性无关向量，如果

$$z\in L(x)\cap L(y)$$

则由$z\in L(x)$可知：$z=ax$，$a\in K$；由$z\in L(y)$可知：$z=by$，$b\in K$，于是得$ax=by$，但因x和y是线性无关的，故可断言：$a=b=0$于是知：$z=\theta$，$L(x)$与$L(y)$交点只能是零向量。

3　证　对于R一模M，有：

$$M=1M\oplus N$$

其中，$1M=\{1x|x\in M\}$是R上的单式模，是M的子模；N是R上的零模，是M的又一个子模。由于M是单模。故只能是$M=1M$或者$M=N$。当$M=N$时，有

$$M=RM=\left\{\sum_{i=1}^{n}r_ix_i\,|r_i\in R,\ x_i\in M,\ \forall n\in N\right\}=\{\theta\}$$

于是加群M的任一真子群都是M的子模，从而由模M的单性可断言加群M也是交换单群。于是可知M只能含有质数个模元素。

当$M=1M$时，是单式模，$M=RM$，于是M只能是循环模。此时，任一非零元皆可作M的生成元。否则$x\neq 0$，$x\in M$又不是M的生成元，那么$Rx\subset M$成为M的真子模，矛盾。

4　证　设$x,y\in N$，则$\forall b\in B$有$bx=\theta$，$by=\theta$于是$b(x-y)=bx-by=\theta$，故$x-y\in N$；又对于rx，$\forall r\in R$，$x\in N$，有

$b(rx)=(br)x=\theta$（因B是右理想，$br\in B$）。从而得知N是M的子模。

5　证　设$x,\ y\in N$，$\forall a\in C$，有$ax=\theta, ay=\theta$，于是$a(x-y)=ax-ay=\theta$，故得$x-y\in N$。对rx，$\forall r\in R$，$x\in N$，有$a(rx)=(ar)x=(ra)x=r(ax)=\theta$，故得$rx\in N$，从而得知：$N$是$M$的子模。

设$a,\ b\in B$，则$\forall x\in M$有$ax=\theta$，$bx=\theta$于是有$(a-b)x=ax-bx=\theta$故$a-b\in B$。又对$\forall r\in R$，$b\in B$有$(rb)x=r(bx)=\theta$，故$rb\in B$，于是知：B是R的左理想。

6　证　设$U=\{u_i\}_{i=1}^{m}$是S的K—基，于是知$\{u_1,u_2,\cdots,u_m\}$是V的m个线性无关向量。从而知：存在$n-m$个向量：$u_{m+1},\ u_{m+2},\ \cdots,\ u_n\in V$使$U'=\{u_i\}_{i=1}^{n}$是$V$的一个$K$—基。$\forall\ \overline{x}\in V/S$

$$\overline{x}=\overline{\sum_{i=1}^{n}a_iu_i}=\sum_{i=1}^{n}a_i\overline{u_i}$$

对于u_i，若$1\leqslant i\leqslant m$，有$u_i\in S$，于是$\overline{u}_i=\overline{\theta}$，故得

$$\overline{x}=\sum_{i=m+1}^{n}a_i\overline{u_i}$$

从而知：$\overline{U'}=\{\overline{u_i}\}_{i=m+1}^{n}$是$V/S$的一个生成集。另外，如果

$$\sum_{i=m+1}^{n}a_i\overline{u_i}=\overline{\theta}$$

则有$\sum\limits_{i=m+1}^{m}a_iu_i\in S$，于是存在$b_1,\ b_2,\ \cdots,\ b_m$使

$$\sum_{i=m+1}^{n}a_iu_i=\sum_{i=1}^{m}b_iu_i$$

由$U'=\{u_i\}_{i=1}^{n}$是V的K—基，故知$a_i=0(i=m+1,\ \cdots,\ n)$。于是断定：$\overline{U}=\{\overline{u_i}\}_{i=m+1}^{n}$是$V/S$的一个$K$—基，$V/S$是$n-m$维

向量空间。

10 证 子模N的商模

$$Z/N=\{\overline{0},\ \overline{1},\ \cdots,\ \overline{p^k-1}\}$$

是Z上p^k元循环模，生成元是$\overline{1}$，于是可知：Z/N 在Z上的子模定是元数为 p^k 约数的循环模。如果 Z/N 存在两个真子模A和 B，A 的元数为 p^i，B的元数为p^j，i，j是小于K的非负整数、且使

$$Z/N=A\oplus B$$

那么必有 $p^k=p^ip^j$，于是知

$$A=L(\overline{p^j})$$

$$B=L(\overline{p^i})$$

如$i\leqslant j$，则 $p^{j-i}\in Z$，于是 $p^{j-i}\overline{p^i}=\overline{p^j}$， 故知： $A\subseteq B$，这与$Z/N=A\oplus B$矛盾。如$i>j$将有$A\supset B$，这也与 $Z/N=A\oplus B$矛盾。故不存在Z/N 的真子模A，B，使$Z/N=A\oplus B$。

11 证（1）如果 $M\neq\{\theta\}$，则M 在R上必存在最小生成集 $U=\{u_i\}_{i=1}^n$，因为 $u_1\in M=AM$，故有

$$u_1=\sum_{i=1}^n a_iu_i,\quad a_i\in A,\ i=1,\ 2,\ \cdots,n$$

于是得

$$(1-a_1)u_1=\sum_{i=2}^n a_iu_i$$

由于 $a_i\in A$，A是真理想，故可断定 $a_1\in B$，于是可知：$1-a_1\overline{\in}B$（否则，$1-a_1=b\in B$，则 $1=a_1+b\in B$， 这与B是真理想矛盾）$(1-a_1)^{-1}\in R$，从而推得

$$u_1=\sum_{i=2}^n(1-a_1)^{-1}a_iu_i$$

这与U是最小生成集矛盾，故 $M=\{\theta\}$。

（2）令$U=\{u_i\}_{i=1}^n$是M的有限生成集，N关于M的商模为

$$M/N=(AM+N)/N$$

$$=\left\{\left(\sum_{i=1}^{n}a_iu_i+n\right)+N \mid a_i\in A,\ u_i\in U,\ n\in N\right\}$$

$$=\left\{\sum_{i=1}^{n}a_i(u_i+N) \mid a_i\in A, u_i\in U\right\}=A(M/N)$$

据（1）可知 $M/N=\{\overline{0}\}$，故得：$M=N$。

§ 7

1　证　设 φ 是 M 上的 R—自同能，$\forall x\in M$，则有 $x=x\cdot 1$，若视 $x\in R$，$1\in M$，那么

$$\varphi(x)=x\varphi(1)$$

于是知 φ 被 $\varphi(1)$ 的值所唯一确定，当 $\varphi(1)=a\in M$ 时，记为 φ_a，则

$$\mathrm{End}_R(M)=\{\varphi_a \mid \varphi_a(1)=a,\ \forall a\in M\}$$

是 M 上的 R—自同态环，令

$$\eta:\ R\longrightarrow \mathrm{End}_R(M),\quad a\longmapsto \varphi_a$$

易证：在 η 下，$R\cong \mathrm{End}_R(M)$。

2　证　令 $\overline{\eta}$：$M/H\longrightarrow M'/H'$

$$\overline{x}=x+H\longmapsto \overline{x}'=\eta(x)+H'$$

易证：在 $\overline{\eta}$ 下，$M/H\cong M'/H'$。

3　（1）$\varphi((a+b)x)=\sigma(a+b)\varphi(x)$

$$=[\sigma(a)+\sigma(b)]\varphi(x)$$

（2）$\varphi((ab)x)=\sigma(ab)\varphi(x)$

$$=(\sigma(a)\sigma(b))\varphi(x)$$

（3）$\varphi(\sigma^{-1}(a)x)=\sigma(\sigma^{-1}(a))\varphi(x)$

$$=a\varphi(x)$$

4　证　由于 $[x]_U=(b_1\ b_2\ \cdots b_n)$ 知：$x=\sum_{i=1}^{n}b_iu_i$ 于是

有：

$$\varphi(x)=\varphi\left(\sum_{i=1}^{n}b_ix_i\right)=\sum_{i=1}^{n}\sigma(b_i)\varphi(u_i)$$

$$=\sum_{i=1}^{n}\sigma(b_i)\left(\sum_{j=1}^{n}a_{ij}u_j\right)$$

$$=\sum_{j=1}^{n}\left(\sum_{i=1}^{n}\sigma(b_i)a_{ij}\right)u_j$$

从而得：

$$[\varphi(x)]_U=\left(\sum_{i=1}^{n}\sigma(b_i)a_{i1},\ \sum_{i=1}^{n}\sigma(b_i)a_{i2},\ \cdots,\right.$$

$$\left.\sum_{i=1}^{n}\sigma(b_i)a_{in}\right)$$

$$=(\sigma(b_1),\sigma(b_2),\cdots,\sigma(b_n))\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&&\vdots\\a_{n1}&a_{n2}&\cdots&a_{nn}\end{pmatrix}$$

$$=[x]_U^{\sigma}A$$

5 解 已知 $v_i=\sum_{j=1}^{n}a_{ij}u_j$，于是得

$$[\varphi(v_i)]_U=[v_i]_U^{\sigma}A=(c_{i1}c_{i2}\ \cdots\ c_{in})^{\sigma}A$$

而

$$[\varphi(v_i)]_V=[\varphi(v_i)]_UC^{-1}=(c_{i1}\ c_{i2}\ \cdots\ c_{in})^{\sigma}AC^{-1}$$

于是得：φ在V上的阵$B=C^{\sigma}AC^{-1}$，其中 $C^{\sigma}=(\sigma(c_{ij}))$。

6 证 （1）$\forall x,\ y\in M$ 有

$$(\varphi\psi)(x+y)=\varphi[\psi(x+y)]=\varphi(\psi(x))+\varphi(\psi(y))$$

$$=(\varphi\psi)(x)+(\varphi\psi)(y)$$

$\forall r\in R,\ x\in M$ 有

$$(\varphi\psi)(rx)=\varphi(\psi(rx))=\varphi(\tau(r)\psi(x))$$

$$=\sigma(\tau(r))\varphi(\psi(x))=(\sigma\tau)(r)(\varphi\psi)(x)$$

于是知：$\varphi\psi$是关于R自同构$\sigma\tau$ 的R一半自同态。

$$(2)\quad (\varphi\psi)u_i=\varphi(\psi(u_i))=\varphi\Big(\sum_{j=1}^{n}b_{ij}u_j\Big)$$

$$=\sum_{j=1}^{n}\sigma(b_{ij})\varphi(u_j)=\sum_{j=1}^{n}\sigma(b_{ij})\Big(\sum_{k=1}^{n}a_{jk}u_k\Big)$$

$$=\sum_{k=1}^{n}\Big(\sum_{j=1}^{n}\sigma(b_{ij})a_{jk}\Big)u_k$$

于是得

$$\mathrm{Mat}_U(\varphi\psi)=\begin{pmatrix}\sum_{j=1}^{n}\sigma(b_{1j})a_{j1} & \sum_{j=1}^{n}\sigma(b_{1j})a_{j2} & \cdots & \sum_{j=1}^{n}\sigma(b_{1j})a_{jn}\\ \sum_{j=1}^{n}\sigma(b_{2j})a_{j1} & \sum_{j=1}^{n}\sigma(b_{2j})a_{j2} & \cdots & \sum_{j=1}^{n}\sigma(b_{2j})a_{jn}\\ \cdots & \cdots & \cdots & \cdots\\ \sum_{j=1}^{n}\sigma(b_{nj})a_{j1} & \sum_{j=1}^{n}\sigma(b_{nj})a_{j2} & \cdots & \sum_{j=1}^{n}\sigma(b_{nj})u_{jn}\end{pmatrix}$$

$$=B^{\sigma}A$$

7　证（1）　令

$$\varphi:\ M\longrightarrow\overline{M},\quad x\longmapsto\overline{x}=x+BM,$$

$$\sigma:\ R\longrightarrow\overline{R}\ r\longmapsto\overline{r}=r+B$$

则φ是M到$\overline{M}$的关于σ的态射，如果$U=\{u_i\}_{i=1}^{n}$是M在R上的生成集，那么$\forall\ \overline{x}\in\overline{M}$，则有$x\in M$使$\varphi(x)=x+BM=\overline{x}$，于是

$$\overline{x}=\varphi(x)=\varphi\Big(\sum_{i=1}^{n}a_iu_i\Big)=\sum_{i=1}^{n}\sigma(a_i)\varphi(u_i)$$

$$=\sum_{i=1}^{n}\overline{a}_i\,\overline{u}_i$$

所以$\overline{U}=\{\overline{u}_i\}_{i=1}^{n}$是$\overline{M}$在$\overline{R}$上的生成集

如果$\overline{U}=\{\overline{u}_i\}_{i=1}^{n}$是$\overline{M}$在$\overline{R}$上的生成集，设$u_i$是$\overline{u}_i$在$\varphi$下的原象之一，作$M$的子模

$$N=\left\{\sum_{i=1}^{n}a_iu_i \mid a_i\in R,\quad i=1,2,\cdots,n\right\}$$

且有

$$\varphi(N)=\{\varphi(x)\mid\forall x\in N\}=\overline{M}$$

于是

$$M=N+\mathrm{Ker}(\varphi)=N+BM$$

据§6习题11可得$M=N$，于是$U=\{u_i\}_{i=1}^n$是M在R上的生成集。

（2）设$U=\{u_i\}_{i=1}^n$是M在R上的最小生成集，则$\varphi(U)=\{\varphi(u_i)\}_{i=1}^n=\{\overline{u}_i\}_{i=1}^n=\overline{U}$是$\overline{M}$在$\overline{R}$上的生成集，也是最小生成集。否则$\overline{U}$中至少有一个向量可被其余向量线性表出，不妨设

$$\overline{u}_1=\sum_{i=2}^{n}\overline{a}_i\overline{u}_i=\sum_{i=2}^{n}\sigma(a_i)\varphi(u_i)$$

$$=\sum_{i=2}^{n}\varphi(a_iu_i)=\varphi\left(\sum_{i=2}^{n}a_iu_i\right)=\varphi(u_1)$$

于是

$$\varphi(u_1-\sum_{i=1}^{n}a_iu_i)=\overline{0}$$

故有

$$u_1-\sum_{i=2}^{n}a_iu_i\in\mathrm{Ker}(\varphi)=BM=\left\{\sum_{i=1}^{n}b_iu_i\mid b_i\in B\right\}$$

从而有

$$u_1-\sum_{i=2}^{n}a_iu_i=\sum_{i=1}^{n}b_iu_i,\quad\forall b_i\in B$$

进而得

$$(1-b_1)u_1=\sum_{i=2}^{n}(a_i+b_i)u_i$$

由$b_1\in B$，B是真理想，可知$1-b_1\overline{\in}B$，$1-b_1$在R中可逆。故得

$$u_1=\sum_{i=2}^{n}(1-b_1)^{-1}(a_i+b_i)u_i$$

这与U是最小生成集矛盾.

由$\overline{U}$是向量空间的最小生成集，故可断言它是一个$\overline{R}$一基。

如果$\overline{U}=\{\overline{u_i}\}_{i=1}^{n}$是$\overline{R}$上向量空间$\overline{M}$的$\overline{R}$一基，设$u_i$是$\overline{u_i}$在$\varphi$下原象之一，$U=\{u_i\}_{i=1}^{n}$是$M$在$R$上的生成集。$\{u_i\}_{i=1}^{n}$必是最小生成集。否则，不妨设$U'\subset U$，是$M$的一个生成集，这时$\overline{U'}\subset\overline{U}$也是$\overline{M}$的生成集，这与$\overline{U}$是$\overline{R}$—基矛盾。

（3）设 $U=\{u_i\}_{i=1}^{n}$、$V=\{v_j\}_{j=1}^{m}$ 是M在R上的两个最小生成集，于是$\overline{U}=\{\overline{u_i}\}_{i=1}^{n}$、$\overline{V}=\{\overline{v_j}\}_{j=1}^{m}$是$\overline{R}$上向量空间$\overline{M}$的两个$\overline{R}$—基。由$\overline{R}$—向量空间$\overline{M}$的维数是唯一确定的，故得：$m=n$。于是断言：$R$一模$M$ 的最小生成集，含有相同个数的模元素。

第五章　扩域习题解答

§1

1 证　设 E 的元素个数为 q，

$$\varphi: a \longmapsto a^p, \quad \forall a \in E$$

考虑 φ 的象 $\mathrm{im}\varphi = \{a^p | a \in E\} \subseteq E$. $\forall a, b \in E, a \neq b$, 有

$$a-b \neq 0, \quad (a-b)^p \neq 0 \text{（因为 } E \text{ 为域）} \quad a^p - b^p \neq 0,$$

$a^p \neq b^p$.

由上述可知：φ 是单射，而且，$\mathrm{im}\varphi$ 也是由 q 个元素组成的集合，于是 $\mathrm{im}\varphi = E$，即 φ 是满射．因此 φ 是 E 到 E 的双射。

另外，$\forall a, b \in E$，有

$$\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$$

综上所述，知 φ 是域 E 的一个自同构．

2 证　（1）由推论 3 知，E 的特征数必是 4 的素约数，而 4 的素约数只有 2，故 E 的特征数为 2．

（2）因 $\mathbf{Z}_p$ 是由 0，1组成的，故 $\forall a \in E$，当 $a \bar{\in} \mathbf{Z}_p$ 时，有 $a \neq 0, 1$．由于 $\{\dot{E};\ \cdot\}$ 是 3 阶有限群，所以 $a^2 \neq 1$，从而 $a \neq a^{-1}$.

显然 $a^{-1} \neq 0, 1$，因此，$E = \{0, 1, a, a^{-1}\}$．考虑 E 中的元素 a^2 和 $a+1$．首先，显然 $a^2 \neq 0, 1, a$，则 $a^2 = a^{-1}$.

其次，$a+1 \neq 0, 1, a$．事实上，如果 $a+1=0$，则因 E 的特征数为 2，而有 $a = -1 = 1$ 矛盾．故 $a+1 \neq 0$．此外显然 $a+1 \neq 1, a$．因此 $a+1 = a^{-1}$，于是 $a^2 = a^{-1} = a+1$．即 a

满足题设方程。

3 证 设E是F所含的最小域. 因E的特征数为p，故由定理2知

$$E\cong \mathbf{Z}_p$$

从而E是由p个元素组成的F的子域. 另一方面

$$x^p-x=0$$

是p次方程，它在域F中的根不会超过p个，而F的每个元素都是它的根，所以F的元素个数不大于p。由于上面证得，F的子域E具有p个元素，故F必是p个元素的域，而且$F=E$.因此

$$F\cong \mathbf{Z}_p$$

4 解 $\mathbf{Z}_p$的特征数为p，$\mathbf{Z}_p$上的有理分式域$\mathbf{Z}_p(x)$就是特征数为p的无限域。

5 解 设 $f(x)=ax^3+bx^2+cx+d$，它是$\mathbf{Z}_2$上三次多项式的一般形式. 由于$\mathbf{Z}_2=\{0, 1\}$，而且$f(x)$的首项系数a只能取$a=1$，其它系数b，c，d各有两种取法，所以$\mathbf{Z}_2$上共有下述$2^3=8$个三次多项式：

$$x^3,\ x^3+1,\ x^3+x,\ x^3+x^2,\ x^3+x+1,\ x^3+x^2+1,$$
$$x^3+x^2+x,\ x^3+x^2+x+1$$

显然$\mathbf{Z}_2$上的三次多项式$f(x)$不可约的充分必要条件是$f(x)$在$\mathbf{Z}_2$中无根. 用$\mathbf{Z}_2$的两个元素0，1逐个代入上述8个多项式，得知在$\mathbf{Z}_2$中无根的只有

$$x^3+x^2+1,\ x^3+x+1$$

它们是$\mathbf{Z}_2$上全部三次不可约多项式。

§2

1 解 因为$\sqrt{5}$，$\sqrt[3]{7}$，i，$i+3$ 分别是有理系数多项式 x^2-5，x^3-7，x^2+1，$x^2-6x+10$的根，所以它们是Q上的代数元。

π^2和$e+3$是Q上的超越元．事实上，假设 π^2 是Q上的代数元，则存在有理系数多项式

$$f(x)=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_0$$

以π^2为根：

$$\begin{aligned}f(\pi^2)&=a_m(\pi^2)^m+a_{m-1}(\pi^2)^{m-1}+\cdots+a_0\\&=a_m\pi^{2m}+a_{m-1}\pi^{2(m-1)}+\cdots+a_0=0\end{aligned}$$

这说明π是有理系数多项式

$$g(x)=a^mx^{2m}+a_{m-1}x^{2(m-1)}+\cdots+a_0$$

的根，与π是Q上的超越元相矛盾．故 π^2是超越元．

假设$e+3$是Q上的代数元，则存在有理系数多项式

$$h(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$

以$e+3$为根：

$$\begin{aligned}h(e+3)&=a_n(e+3)^n+a_{n-1}(e+3)^{n-1}+\cdots+a_0\\&=a_n(e^n+C_n^13e^{n-1}+\cdots+3^n)\\&\quad+a_{n-1}(e^{n-1}+C_{n-1}^13e^{n-2}+\cdots+3^{n-1})\\&\qquad\vdots\\&\quad+a_0\\&=a_ne^n+(a_nC_n^13+a_{n-1})e^{n-1}+(a_nC_n^23^2+\\&\quad a_{n-1}C_{n-1}3+a_{n-2})e^{n-2}+\cdots\\&\quad+(a_n3^n+a_{n-1}3^{n-1}+\cdots+a_0\\&=0\end{aligned}$$

这说明e是有理系数多项式

$$\begin{aligned}k(x)=a_nx^n+(a_nC_n^13+a_{n-1})x^{n-1}+(a_nC_n^23^2\\+a_{n-1}C^1_{n-1}3+a_{n-2})x^{n-2}+\cdots+h(3)\end{aligned}$$

的根，与e是Q上的超越元相矛盾．故$e+3$是超越元．

2　证　在1题的证明的后一部分，把π和e都换成α，便得到本题充分性的证明．现证明必要性．

设α是Q上的代数元，Q上的多项式

$$\varphi(x)=x^n+a_1x^{n-1}+\cdots+a_n$$

以α为根，设$\varphi(x)$的全部根是$\alpha_1=\alpha$，α_2，…，α_n．由高等代

数知，每个a_i都是$\alpha_1, \alpha_2, \cdots, \alpha_n$的初等对称多项式。考虑下述两个多项式：

$$f_1(x) = (x-\alpha_1^2)(x-\alpha_2^2)\cdots(x-\alpha_n^2)$$
$$= x^n + b_1x^{n-1} + \cdots + b_n$$
$$f_2(x) = (x-(\alpha_1+3))((x-(\alpha_2+3))\cdots(x-(\alpha_n+3))$$
$$= x^n + c_1x^{n-1} + \cdots + c_n$$

$f_1(x), f_2(x)$的根分别是$\alpha_1^2, \alpha_2^2, \cdots, \alpha_n^2$和$\alpha_1+3, \alpha_2+3, \cdots, \alpha_n+3$。$f_1(x), f_2(x)$的每个系数$b_i$和$c_i$分别是$\alpha_1^2, \alpha_2^2, \cdots, \alpha_n^2$和$\alpha_1+3, \alpha_2+3, \cdots, \alpha_n+3$的初等对称多项式，也都是$\alpha_1, \alpha_2, \cdots, \alpha_n$在$Q$上的对称多项式。由对称多项式基本定理，$b_i$和$c_i$都可表成$\alpha_1, \alpha_2, \cdots, \alpha_n$的初等对称多项式$a_1, a_2, \cdots, a_n$在$Q$上的多项式：

$$b_i = g_i(a_1, a_2, \cdots, a_n), \quad c_i = q_i(a_1, a_2, \cdots, a_n)$$

由于每个a_i都是有理数，所以b_i和c_i也都是有理数，即$f_1(x)$和$f_2(x)$都是Q上的多项式。它们分别以$\alpha_1^2 = \alpha^2$和$\alpha_1 + 3 = \alpha + 3$为根，因此$\alpha^2$和$\alpha+3$都是$Q$上的代数元。必要性得证。

3　证　设A是S的任一有限子集，则$F(A)$是$F(S)$的子域，设

$$\Sigma = \{F(A) \mid A \subseteq S, A\text{是有限集合}\}, \quad F' = \bigcup_{F(A)\in\Sigma} F(A)$$

显然$F' \subseteq F(S)$。另一方面，$\forall \alpha \in F(S)$，有

$$\alpha = \frac{f(\alpha_1, \alpha_2, \cdots, \alpha_n)}{q(\alpha_1, \alpha_2, \cdots, \alpha_n)}, \quad \alpha_i \in S, \quad q(\alpha_1, \alpha_2, \cdots, \alpha_n) \neq 0$$

但$\alpha \in F(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \Sigma$，故$\alpha \in F'$，即$F(S) \subseteq F'$。因此$F' = F(S)$，于是$F'$是一个域。

4　证　设$f(x) \in F[x]$是α的最小多项式，由命题2知

$$f(x) \mid \varphi(x)$$

因$\varphi(x)$是不可约多项式，故$f(x)$与$\varphi(x)$的次数相等，于是

$$f(x) = c\varphi(x), \quad c \in F$$

但$f(x)$，$\varphi(x)$的首项系数都是1，所以$c=1$，即$f(x) = \varphi(x)$，

$\varphi(x)$是α的最小多项式。

5 解 $C=R(i)$，而$\varphi(x)=x^2+1$是以i为根的实系数多项式，且$\varphi(x)$在R上不可约，故$\varphi(x)=x^2+1$是i在R上的最小多项式。

$f(x)=x^5-3$是以$\sqrt[5]{3}$为根的有理系数多项式，用艾森斯坦因判别法可以判定$f(x)$是Q上不可约多项式，故$f(x)=x^5-3$是$\sqrt[5]{3}$在Q上的最小多项式。

§ 3

1 证 由于

$$\Delta(x)=F\left(\frac{x^3}{x+1}\right)(x)=F(x)=\Sigma$$

所以Σ是Δ的单纯扩张。现证明添加元x是$\Delta=F\left(\frac{x^3}{x+1}\right)$上的代数元。

令 $y=\frac{x^3}{x+1}\in\Delta$，显然$y\in\Sigma$，则在$\Sigma=F(x)$中有

$$y(x+1)=x^3,\quad x^3-yx-y=0$$

这说明x是Δ上的三次多项式

$$\varphi(z)=z^3-yz-y$$

的根。故x是Δ上的代数元，从而$\Sigma=\Delta(x)$是Δ的单纯代数扩张。

2 解（参看第五章§3学习指导(二)中的3）$\sqrt[3]{2}$在Q上的最小多项式为$\varphi(x)=x^3-2$。设

$$\alpha=\frac{f(\sqrt[3]{2})}{g(\sqrt[3]{2})}=\frac{1+\sqrt[3]{2}}{1+\sqrt[3]{2}+\sqrt[3]{4}}$$

则 $f(x)=x+1$，$g(x)=x^2+x+1$。用带余除法求得 $u(x)=x-1$，$v(x)=-1$，使

$$g(x)u(x)+\varphi(x)v(x)=1$$

于是

$$(g(\sqrt[3]{2}))^{-1}=u(\sqrt[3]{2})=\sqrt[3]{2}-1$$

故

$$\begin{aligned}\alpha&=f(\sqrt[3]{2})(g(\sqrt[3]{2}))^{-1}\\&=(\sqrt[3]{2}+1)(\sqrt[3]{2}-1)\\&=(\sqrt[3]{2})^2-1\end{aligned}$$

3　解　因$g(x)=x^2+x+1$的判别式 $b^2-4ac=1-4\times1\times1=-3<0$，故$g(x)$在$R$上不可约。所以 $g(x)$ 是 α 在R上的最小多项式，其次数为 2，则

$$R(\alpha)=\{c\alpha+d\mid c,\ d\in R\}$$

由于 $g(x)$在 $R(\alpha)$中有根 α，故 $g(x)$在 $R(\alpha)$上有因式$x-\alpha$。以$x-\alpha$除$g(x)$得商式$x+\alpha+1$，所以$g(x)$在$R(\alpha)$上可分解成两个一次多项式之积：

$$g(x)=(x-\alpha)(x+\alpha+1)$$

4　解　（1）假设y^p-x在K上可约，则存在K上$m<p$次不可约多项式$\varphi(y)$，使得 $\varphi(y)\mid y^p-x$。于是存在K的单纯代数扩张$K(\alpha)$，使α在K上的最小多项式为 $\varphi(y)$。由于 $\varphi(y)\mid y^p-x$，故α是y^p-x的根：

$$\alpha^p-x=0,\ \alpha^p=x,\ \alpha=x^{\frac{1}{p}}\ .$$

从而在$K(\alpha)$上，

$$y^p-x=y^p-\alpha^p=(y-\alpha)^p=(y-x^{\frac{1}{p}})^p$$

因此

$$\varphi(y)=(y-x^{\frac{1}{p}})^m$$

但 $\varphi(y)$ 是K上的多项式，其常数项 $(-1)^m x^{\frac{m}{p}}$ 应属于 $K=F(x)$。因为 $m<p$，所以这是不可能的。因此 y^p-x在K上不可约。

（2）由于添加元θ的最小多项式 y^p-x的次数为p，所以

$$K(\theta)=\left\{\sum_{i=0}^{p-1}h_i\theta^i\mid h_i\in K\right\}$$

（因为 $K=F(x)$），其中，$h_i=\dfrac{f_i(x)}{g_i(x)}$，$f_i(x)$，$g_i(x)\in F[x]$，

$g_i(x) \neq 0$。

由于 θ 是 $y^p - x$的根，所以

$$\theta^p - x = 0, \quad x = \theta^p$$

于是 $\forall \alpha \in K(\theta)$ 有

$$\alpha = \sum_{i=0}^{p-1} h_i \theta^i = \sum_{i=0}^{p-1} \frac{f_i(x)}{g_i(x)} \theta^i$$

$$= \sum_{i=0}^{p-1} \frac{f_i(\theta^p)}{g_i(\theta^p)} \theta^i \in F(\theta)$$

即

$$K(\theta) \subseteq F(\theta)$$

另一方面，显然有 $F(\theta) \subseteq K(\theta)$。因此

$$K(\theta) = F(\theta)$$

（3）因为 $x = \theta^p$，同时 $K(\theta)$ 的特征数为 p，所以在 $K(\theta)$上有

$$y^p - x = y^p - \theta^p = (y - \theta)^p$$

这就是$y^p - x$在$K(\theta)$上的标准分解式。

§ 4

1　证　因 α 在 F 上的最小多项式的次数为 m，故 $F(\alpha)$ 是 F 的 m 次扩张，$F(\alpha) \subseteq K$。由于 K 是 F 的 n 次有限扩张，则由定理 3 有

$$K = F(\alpha_1, \alpha_2, \cdots, \alpha_S)$$

其中α_i是 F 上的代数元。显然

$$F(\alpha)(\alpha_1, \alpha_2, \cdots, \alpha_S) = K$$

即 K 也是 $F(\alpha)$ 的有限扩张，令$\left(\frac{K}{F(\alpha)}\right) = m'$，由定理 1 知

$$mm' = n$$

故 $m|n$。

2　证　因E是F的有限扩张，由定理2知，E是F的代数扩张，故$\alpha \in E$是F上的代数元。于是$F(\alpha)$是F的单纯代数扩张。而$(F(\alpha)/F)=m$等于α在F上的最小多项式次数。由1题得$m|n$。

3　解　由于

$$Q(i,\sqrt{2})=Q(i)(\sqrt{2})$$

而且，i在Q上的最小多项式为x^2+1，则

$$(Q(i)/Q)=2$$

$\sqrt{2}$在$Q(i)$上的最小多项式为x^2-2，则

$$(Q(i)(\sqrt{2})/Q(i))=2$$

故由定理1得

$$(Q(i,\sqrt{2})/Q)=(Q(i)/Q)(Q(i)(\sqrt{2})/Q(i))$$
$$=2\times 2=4$$

4　证　设$\alpha_1, \alpha_2, \cdots, \alpha_n$是$K$在$Z_p$上的基底，于是$K$中任一元素$\alpha$可被$\alpha_1, \alpha_2, \cdots, \alpha_n$在$Z_p$上唯一地线性表出：

$$\alpha=a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n, \quad a_i \in Z_p$$

这里每个a_i都有p种取法，所以恰好可做出p^n组表示系数，于是K是p^n个元素组成的有限域。

5　证　因为α是K上的代数元，所以$K(\alpha)$是K的单纯代数扩张，从而是K的有限扩张。而K是F的有限扩张，由定理1知，$K(\alpha)$是F的有限扩张。再由定理2知，$K(\alpha)$中的元素α是F上的代数元。

§ 5

1　解　求得$f(x)=x^3-5x^2+9x-9$的根为

$$x_1=3, \quad x_2=1+\sqrt{-2}, \quad x_3=1-\sqrt{-2}$$

则$f(x)$在Q上的分裂域为

$$Q(x_1,x_2,x_3)=Q(\sqrt{-2})$$

2　证　由于a是$\varphi(x)=x^3-a$的根，则$\alpha\omega^0$，$\alpha\omega$，$\alpha\omega^2$是

$\varphi(x)$的全部根，其中ω是三次本原单位根：

$$\omega = \frac{-1+\sqrt{3}i}{2}$$

假设$Q(\alpha)$是$\varphi(x)$的分裂域，则 $\alpha\omega \in Q(\alpha)$，从而

$$\omega \in Q(\alpha)$$

于是有

$$Q \subset Q(\omega) \leqslant Q(\alpha)$$

由定理1，$(Q(\omega)/Q)$应该是$(Q(\alpha)/Q)$的约数.但是ω在 Q 上的最小多项式为x^2+x+1，则

$$(Q(\omega)/Q)=2$$

而α在Q上的最小多项式为$\varphi(x)=x^3-a$，有

$$(Q(\alpha)/Q)=3$$

$(Q(\omega)/Q)$不是$(Q(\alpha)/Q)$的约数.这个矛盾说明$Q(\alpha)$不是$\varphi(x)$在 Q上的分裂域.

3　证　设$\varphi(x)=\varphi_1(x)\varphi_2(x)\cdots\varphi_m(x)$. 显然 $\varphi(x)$是F上的多项式，由定理1，存在 $\varphi(x)$在F上的分裂域K. 因为K包含 $\varphi(x)$ 的全部根，所以K包含每个$\varphi_i(x)$的全部根. 在K中取$\varphi_i(x)$的根α_i，$i=1,2,\cdots,m$.显然每个α_i 都是F上的代数元，于是在K中，将K的子集$\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$添加到$F$上，得到$F$的有限扩张$F(\alpha_1, \alpha_2, \cdots, \alpha_m)$. 由于每个$\varphi_i(x)$都是首项系数为1的不可约多项式，所以 α_i 在F上的最小多项式为$\varphi_i(x)$.

4　证　对多项式$f(x)$的次数用数学归纳法.

当$n=1$，此时$f(x)$是F上不可约多项式，是其唯一根α_1在F上的最小多项式，故 $f(x)$的分裂域 $E=F(\alpha_1)$关于F的次数为$1=1!$.

假设命题对$n-1$成立. 令$\alpha_1, \alpha_2, \cdots, \alpha_n$是$f(x)$在其分裂域$E$中的$n$个根，则$E=F(\alpha_1, \alpha_2, \cdots, \alpha_n)$. 现考虑$E$的子域$F(\alpha_1)$. 显然$\alpha_1$在$F$上的最小多项式的次数$\leqslant n$，则

$$(F(\alpha_1)/F) \leqslant n \qquad (1)$$

在$F(\alpha_1)$上，$f(x)$可分解为

$$f(x)=(x-\alpha_1)\varphi(x)$$

其中$\varphi(x)$是$F(\alpha_1)$上的$n-1$次多项式，而且α_2，…，α_n恰好是$\varphi(x)$在K中的所有$n-1$个根。由归纳假设，$\varphi(x)$在$F(\alpha_1)$上的分裂域$F(\alpha_1)(\alpha_2, \cdots, \alpha_n)$关于$F(\alpha_1)$的次数

$$(F(\alpha_1)(\alpha_2, \cdots, \alpha_n)/F(\alpha_1))\leqslant(n-1)! \qquad (2)$$

将不等式（1）和（2）的两端分别相乘得

$$(F(\alpha_1, \alpha_2, \cdots, \alpha_n)/F)=(F(\alpha_1)/F)(F(\alpha_1)(\alpha_2, \cdots, \alpha_n)/F(\alpha_1))\leqslant n(n-1)!\ )=n!$$

§ 6

1 证 设

$$\dot{E}=\{\alpha_1, \alpha_2, \cdots, \alpha_{q-1}\}$$

由定理4的证明中得知，$\dot{E}$恰是由Z_p上所有$q-1$次单位根组成的。于是

$$x^{q-1}-1=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{q-1})$$

其中$q=p^n$。现在比较上式两端的常数项：

当$p=2$时，有$1=-1$，而$q-1=p^n-1$是奇数，则

$$\alpha_1\alpha_2\cdots\alpha_{q-1}=1=-1$$

当$p\neq 2$时，$q-1=p^n-1$是偶数，则

$$\alpha_1\alpha_2\cdots\alpha_{q-1}=-1$$

2 证 设

$$f(x)=a_m x^m+a_{m-1}x^{m-1}+\cdots+a_0, \quad a_i\in Z_p$$

Z_p的元素个数为p，由定理2的证明中得知，Z_p中的元素都是多项式

$$x^p-x$$

的根，所以对于每个a_i均有

$$a_i^p=a_i$$

于是

$$f(\alpha^p) = a_m(\alpha^p)^m + a_{m-1}(\alpha^p)^{m-1} + \cdots a_0$$
$$= a_m^p(\alpha^m)^p + a_{m-1}^p(\alpha^{m-1})^p + \cdots + a_0^p$$
$$= (a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0)^p$$
$$= (f(\alpha))^p = 0$$

因此α^p是$f(x)$的根。同理可得

$$f(\alpha^{p^2}) = (f(\alpha^p))^p = 0$$
$$\vdots$$
$$f(\alpha^{p^m}) = (f(\alpha^{p^{m-1}}))^p = 0$$

所以 α^{p^2}, …, α^{p^m}也都是 $f(x)$的根。

3 解 因为 $4 = 2^2$，所以4元有限域的特征数为2，是$\mathbf{Z}_2$的二次扩张。

考虑 $\mathbf{Z}_2 = \{0, 1\}$上的二次多项式

$\varphi(x) = x^2 + x + 1$

由于0,1都不是 $\varphi(x)$的根，则$\varphi(x)$是 $\mathbf{Z}_2$上的不可约多项式。由§3定理3，存在 $\mathbf{Z}_2$ 的单纯代数扩张

$F = \mathbf{Z}_2(\alpha)$

其中 α 在$\mathbf{Z}_2$上的最小多项式为 $\varphi(x) = x^2 + x + 1$。因$(F/\mathbf{Z}_2) = 2$，则F的元素个数为 $2^2 = 4$。

F的任一元素可表为

$a\alpha + b$, $a, b \in \mathbf{Z}_2$

a，b各有两种取法，于是F的四个元素是：0,1, α, $\alpha+1$。其加法表和乘法表如下：

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

·	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

4　**证**　由§1习题1的证明得知，$\forall \alpha \in E$，存在 $a \in E$ 使得

$$\alpha = a^p$$

即 E 中存在 α 的 p 次方根。

假设 $a, b \in E$ 都是 α 的 p 次方根：

$$\alpha = a^p = b^p$$

则 $a^p - b^p = 0$，$(a-b)^p = 0$，$a - b = 0$，$a = b$。故 α 在 E 中的 p 次方根是唯一的。

附录　参考书目

代数学　B. L. 范德瓦尔登著丁石孙等译　科学出版社1963年。

抽象代数学　N. 贾柯勃逊著黄缘芳译　科学出版社1960年。

近世代数　熊全淹编著　上海科技出版社1978年。

近世代数基础　张禾瑞著　人民教育出版社1978年。

近世代数　吴品三编　人民教育出版社1979年。

近世代数概论　G. 伯克霍夫、S. 麦克莱恩著王连祥、徐广善译　人民教育出版社1979年。

后　记

本书由高绪珏主编。第一章与第五章由孙保民编写，第二章由杨慧编写，第四章由邹立国编写。

本书承蒙辽宁大学数学系陈继普副教授，仔细地审阅了原稿，并提出了许多宝贵意见，在此谨致谢意。

限于编者水平，书中不妥或谬误之处，欢迎读者批评指正。

编者

1983年12月

［Ｇｅｎｅｒａｌ　Ｉｎｆｏｒｍａｔｉｏｎ］
书名＝近世代数
作者＝
页数＝４６８
ＳＳ号＝０
出版日期＝
Ｖｓｓ号＝５６６３１５９９

封面
书名
版权
前言
目录

目　　录

第一部分近世代数
第一章基本概念
§１　　集合
§２　　映射
§３　　商集与等价关系
§４　　代数体系
§５　　同态　　同构
§６　　半群　　亚群
第二章群
§１　　群的定义
§２　　子　　群
§３　　群的同态、同构
§４　　循环群
§５　　变换群　　置换群
§６　　子群的陪集
§７　　正规子群与商群
§８　　群的同态基本定理
§９　　直和
第三章环与域
§１　　环的定义
§２　　整环、除环和域
§３　　子　　环
§４　　矩阵环
§５　　理想与商环（差环）
§６　　环的同态与同态基本定理
§７　　极大理想与素理想
§８　　商域
§９　　多项式环
§１０　　整环和域上的多项式环
§１１唯一分解环
第四章模
§１　　模的定义
§２　　模的生成集
§３　　自由模
§４　　ｎ秩自由模上的线性代数
§５　　向量空间上的线性代数
§６　　子模和商模
§７态射
第五章扩域
§１　　特征数素域

§ 2 扩张
§ 3 单纯扩张
§ 4 有限扩张
§ 5 分裂域
§ 6 有限域
第二部分近世代数学习指导
第一章基本概念学习指导
第二章群学习指导
第三章环与域学习指导
第四章模学习指导
第五章扩域学习指导
第三部分近世代数习题解答
第一章基本概念习题解答
第二章群习题解答
第三章环与域习题解答
第四章模习题解答
第五章扩域习题解答
附录
后记